Automating interpretations of trustworthiness

Submitted by

Marc Sel

for the degree of Doctor of Philosophy

of

Royal Holloway, University of London

2021

Declaration

I, Marc Sel, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Marc Sel (Signature)

Digitally signed by Marc Sel (Signature)
Date: 2021.07.27 16:48:28 +02'00'

Signed . . . . . (Marc Sel)
Date:

To Trijntje.

Abstract

Digital services have a significant impact on the lives of many individuals and organisations. Trust influences decisions regarding potential service providers, and continues to do so once a service provider has been selected. It is common to refer to the entity that is trusting as the trustor, and to the entity that is trusted as the trustee. There is no globally accepted model to describe trust in the context of digital services, nor to evaluate the trustworthiness of entities. Trust is commonly used in the context of digital services, yet it is overloaded with meaning and difficult to interpret.

This thesis presents a novel model to describe and evaluate an entity's trustworthiness. The model is referred to as the trustworthy ecosystem model. It is based on four building blocks: a data model, a rulebook, trustworthiness evaluation functions and instance data.

The data model is expressed in First Order Logic. Rulebooks, which consist of constraints that reflect a particular context for reasoning about trustworthiness, are described using predicates. The entity that is evaluating is referred to as the evaluator, and the entity that is evaluated is the evaluation subject. The evaluator corresponds to a potential trustor, and the evaluation subject to a potential trustee.

Verifying whether the constraints are satisfied over a set of instance data allows an evaluator to evaluate the trustworthiness of an evaluation subject. For this purpose trustworthiness evaluation functions are specified. The functions takes as input a rulebook, i.e. a set of constraints, and a set of data. A rulebook contains a mandatory and a discretionary part. The mandatory part describes the constraints that must be satisfied to have the minimal basis for relevant execution of the discretionary rules. The discretionary part allows the evaluator to specify a trustworthiness evaluation policy by selecting discretionary constraints. The data represents real world information about the potential trustee and its context. The outcome of the evaluation provides evidence that can be used by the evaluator to decide to interact with the evaluation subject in the relationship of trustor–trustee.

To demonstrate the practical feasibility of the proposed framework, a partial implementation is presented. The data model was implemented in OWL, a logic language that was established by the Worldwide Web Consortium (W3C). The data model was complemented by a data import and transformation mechanism which transforms data from public and authoritative sources into the data model and stores it in a graph database. A sample rulebook and trustworthiness evaluation function were implemented in the form of SPARQL queries. The implementation is partial because it implements only two particular rulebooks, inspired by the European legislation for trust services, and because it uses a specific set of data sources for its instance data.

The approach was validated by implementing the model, importing real world data, performing selective evaluations of trustworthiness and comparing their outcome to other ap-

proaches such as PKI and the Web of Trust verification.

The scientific contribution of the thesis can be summarised as follows:

- A thorough investigation of the current academic field on trust and trustworthiness was performed through a literature review, to identify potential improvement points and thus create the basis for the thesis.
- An integrated set of requirements for trust, i.e. things which must hold for an entity, or the outcome of an interaction to be regarded as trustworthy, were proposed on the basis of the literature review and the findings of the FutureTrust research project.
- Based on these requirements, a new way to logically model providers and consumers of digital services as well as the providers of trust services as participants in a digital ecosystem was proposed. It is based on a data model, a rulebook, trustworthiness evaluation functions and instance data.
- A partial implementation of the model was performed to validate it, using data from authoritative public sources.

Acknowledgements

I am very grateful to Professor Chris Mitchell, for being my Supervisor and keeping me on track. His comments were always a wonderful balance in terms of shortness, being to the point and being constructive. He introduced me to the academic world in a fantastic way. Thank you so much, Chris. You were an extraordinary guide.

I'm also grateful to Professor Jason Crampton for challenging and supporting me as Advisor. I have really enjoyed every talk, comment and discussion. Thank you so much, Jason.

Furthermore, I have to thank Professor Bart Preneel for planting the seed of my curiosity in security and cryptology. And I thank Professor Stephen Marsh for making me feel welcome at various IFIP International Conferences on Trust Management, which provided a challenging breeding ground, and Professor Vijay Varadharajan for interesting discussions. My special thanks go to Detlef and Tina Hühnlein for inviting me to join the inspiring FutureTrust project. Professor Jörg Schwenck as well as Vladimir Mladenov and Juraj Somorovsky are thanked for their friendly collaboration and the exchange of ideas, as well as Herbert Leitold, Thomas Zefferer, Gerald Dißauer, Elif Üstündağ Soykan and Edona Fasllija. I am also indebted to Nikos Loutas for his motivating introduction to the semantic web. Finally I thank Danny De Cock for stimulating discussions.

This work was conducted using the Protégé and GraphDB resources. Protégé[1] is supported by grant GM10331601 from the National Institute of General Medical Sciences of the United States National Institutes of Health. Ontotext offered free use of their GraphDB database[2].

[1] `https://protege.stanford.edu/`

[2] `https://www.ontotext.com/products/graphdb/`

Contents

List of Figures

List of Tables

Listings

List of Notation

β	rulebook
β_{AE}	example rulebook for the evaluation of an ecosystem
β_{AP}	example rulebook for the evaluation of a participant
AB	Accreditation Body
Agreement	predicate of the form *Agreement(p_{id}, r_{id}, [t_m], [c_m])* where p_{id} stands for the participant that agrees to be bound by the rulebook r_{id} stands for the rulebook t_m stands for an optional time mark c_m stands for an optional commitment mark
Attestation	predicate of the form *Attestation(p_{id}, T, [t_m], [c_m])* where p_{id} stands for the issuer of the attestation T stands for the triple (subject, attribute, value) that makes up the core information of the attestation, where t_m stands for an optional time mark c_m stands for an optional commitment mark
$\mathcal{A}ttestation_{p_{id}}()$	projection function on Attestation that allows the selection of its issuer
$\mathcal{A}ttestation_{t_{att}}()$	projection function on Attestation that allows the selection of the triple's attribute
$\mathcal{A}ttestation_{t_{sub}}()$	projection function on Attestation that allows the selection of the triple's subject
$\mathcal{A}ttestation_{t_{val}}()$	projection function on Attestation that allows the selection of the triple's attribute value
$\mathbb{C}$	allowed character set, unless specified otherwise it corresponds to the Latin alphabet defined in ISO/IEC 8859-1:1998 [182] with permitted sub and superscripting for readability
$\mathcal{C}$	claim identification set
Claim	predicate of the form *Claim(c_{id}, r_{id}, c_{cla}, S_e, claimstate, [t_m], [c_m])*

	where c_{id} and r_{id} stand for the identification of the claim and the applicable rulebook, and S_e stands for the set of evidence for which *claimstate* is claimed by the claimant c_{cla}
c_m	commitment mark, optional set of attributes that express commitment of the creator
CsSP	claim status service provider, a participant that provides status information about a claim
$\mathcal{E}$	evidence identification set
EnDo	endorser, a participant that proposes and supports a rulebook
Endorsement	predicate of the form *Endorsement(p_{id}, r_{id}, [t_m], [c_m])*
EnFo	enforcer, a participant that enforces (rejects/confirms) claims
Enforcement	predicate of the form *Enforcement(p_{id}, r_{id}, [t_m], [c_m])*
Evidence	predicate of the form *Evidence(e_{id}, i_{id}, e_{evsp}, S_{sav}, [t_m], [c_m])* where S_{sav} consists of (subject, attribute, value) triples
EvSP	evidence service provider, a participant that provides evidence services to interacting participants
$f_{comcreate}(p_{id}, predicate)$	commitment creation function where (p_{id}) is the invoking participant, *predicate* is what (p_{id}) wants to commit
$f_{comprep}(p_{id1},p_{id2})$	commitment preparation function where (p_{id1}) is the invoking participant, (p_{id2}) is the participant whose commitment can be created and can be verified using the commitment validation data returned in the form *CVD(p_{id1}, (p_{id2}, commitment-validation-data, data))*
$f_{comverif}(A, CVD())$	commitment verification function of the form $f_{comverif}$(A, CVD(p_{id1}, (p_{id2}, commitment-validation-data, data))) which verifies the predicate A's time and commitment mark, returning true if the verification was successful and false otherwise
f_{ia}	property attestation function for identity attributes
f_{ra}	property attestation function for role attributes
f_{re}	rulebook endorser attestation function
f_{ga}	property attestation function for general attributes
FOL	first order logic
FuSC	functional service consumer

FuSP	functional service provider
$\mathcal{I}$	interaction identification set
Interaction	participant interaction of the form *Interaction*(i_{id}, S_{ip}, *information, cre)* where S_{ip} stands for the interaction's participants and *information* stands for a (possibly empty) string representing information transferred or stored/retrieved
$\mathcal{P}$	participant identification set
$\mathcal{R}$	rulebook identification set
S_A	set of all actors
S_{abr}	set of all base role attestations
S_{aio}	set of attributes for identity of organisations
S_{aip}	set of attributes for identity of natural persons
S_{ag}	set of general attributes, equal to {seq $\mathbb{C}$} with $\mathbb{C}$ as the allowed characterset
S_{agr}	set of all agreements
S_{arb}	set of all base roles, equal to { R_{FuSP}, R_{FuSC}, R_{EnDo}, R_{EnFo}, R_{AB}, R_{EvSP}, R_{CsSP}
S_{attn}	set of all attestations
S_{cla}	set of all claim predicates
S_{ds}	set of all data sources
S_e	set of evidence predicates embedded within a claim
S_{end}	set of all endorsements
S_{evi}	set of all evidence predicates
S_{int}	set of all interaction predicates
S_{ip}	set of participants in an interaction
S_{PT}	set of all participants
S_R	set of all rulebooks
S_{sav}	set of (subject, attribute, value) triples
S_{SOD_1}	first segregation of duty set, equal to { R_{EvAA}, R_{EvSPMo}, R_{CsAA}, R_{CsSPMo} }
S_{SOD_2}	second segregation of duty set, equal to { R_{EnDo}, R_{EnFo}, R_{FuSP}, R_{FuSC} }
S_{sup}	set of all supervision attestations
$\mathcal{TE}$	trustworthy ecosystem
t_m	time mark, optional set of attributes that express time of creation (*cre*), start of validity (*sov*), and end of validity (*eov*)

$twseval_{AE}$	trustworthiness evaluation function for an ecosystem
$twseval_{AP}$	trustworthiness evaluation function for a participant

List of Abbreviations

AB	Accreditation Body
AS	Authentic Source
CA	Certification Authority
CAB	Conformity Assessment Body
CsSP	Claim Status Service Provider
EnDo	Endorser
EnFo	Enforcer
EvSP	Evidence Service Producer
FuSC	Functional Service Consumer
FuSP	Functional Service Producer
GDPR	General Data Protection Regulation
ICAO	International Civil Aviation Organisation
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IRI	Internationalised Resource Identifier
PKI	Public Key Infrastructure
QTSP	Qualified Trust Service Provider
SB	Supervisory Body
TSP	Trust Service Provider
TTP	Trusted Third Party
TwsMo	Trustworthiness Monitor
URI	Uniform Resource Identifier
WOT	Web of Trust

Chapter 1

Introduction

This chapter describes the motivation and methodology for the work described in this thesis, and specifies the research challenges that have been addressed. The scientific contributions and the publications that resulted from the work are summarised. Finally, an outline of the thesis, which consists of three main parts, is given.

1.1 Motivation

1.1.1 The importance of trust

Electronic platforms have a significant impact on the lives of many. On some platforms, predators can pose as a 14-year-old girl. More often than not, such platforms are operated by for-profit giants, performing unknown functions in an unknown manner. The algorithms used by search engines and their relationship with advertising agencies are not always disclosed. Nevertheless, for a variety of reasons, users often trust such services.

Trust is important because its presence or absence can have a strong influence on what we choose to do or not do, both as an individual and as a group. Trust decisions are made by all of us, and today automata are increasingly confronted with such decisions. Each time a trust decision is made, something is put at risk. It may be a human life, an animal or a material thing. Trust decisions are based on a mixture of experience and expectation. The one that is trusting is commonly referred to as the trustor, the one that is trusted is the trustee. The trustee may or may not live up to the trustor's expectation. Betrayal of trust is the responsibility of the trustee, not of the trustor. The negative consequences of betrayal of trust may, however, impact the trustor.

Trust has been extensively studied from many perspectives. In the social sciences, trust is discussed from a number of different points of view. A thorough treatment can be found

for example in the work of Deutsch [70]. Trust, as studied from the social point of view, is a complex subject from which a rich terminology has emerged. This terminology has influenced the study of trust in an information technology context where, unfortunately, the terms trust and trustworthiness are far from having a common definition or interpretation, as pointed out below.

1.1.2 The meaning of trust

It is important to consider the meaning of the terms trust and trustworthiness, and how to interpret claims of trust and of trustworthiness, because these terms are commonly used in the field of information technology without a precise definition or agreement on their meaning. The following definitional issues are particularly significant, and are discussed in greater detail below.

- There is a lack of clarity in, and agreement on, the meaning of the term trust. Despite this, technology dependent on the notion of a trusted third party, such as Public Key Infrastructure (PKI) schemes, are widely used.
- The term trust is ambiguous, as it is used as both a positive and a negative characteristic.
- The terms trust and trustworthiness are used with different meanings in Europe and in the United States of America.
- Various initiatives have attempted to provide an agreed meaning for trust, but they have so far had limited effect.

1.1.3 Lack of clarity

High-level definitions of trust exist, such as those of Castelfranchi and Francone [46], Gambetta et al. [119] and Cofta [62]. Castelfranchi and Francone [46] state that *'trust is in fact a deficiency of control that expresses itself as a desire to progress despite the inability to control'*. This can be paraphrased as *'trust is accepted dependence'*. This idea is elaborated by Gollmann [131], who argues that it would be generally helpful if authors avoided references to trust. Trust is a natural term to use in psychology but not in computer science. He provides examples of the use of the terms trust and trustworthiness, including the following.

- A Trusted Computing Base (TCB) is defined according the Trusted Computer System Evaluation Criteria [322] in 1985 as 'the totality of protection mechanisms within a computer system — including hardware, firmware, and software -– the combination of which is responsible for enforcing a security policy.' Using this terminology, if a trusted component fails, security can be violated, i.e. trusted components are those that can hurt you.

Components that signal errors and unexpected behaviour, i.e. that come with evidence of their failure, are called trustworthy.

- Code-based access control has been proposed as an alternative to identity-based schemes [132]. In code-based access control, access privileges are assigned to code, not to users. It is customary to refer to code running with many privileges as trusted code and to code running with few privileges as untrusted code. A flaw in code running with system privileges might be exploited by an attacker. The same flaw in code that runs with limited privileges would have less serious implications. In this sense, trusted (privileged) code is a component that can hurt you. However, calling code trusted may also insinuate that this is code you can trust, i.e. trustworthy code, which can easily lead to confusion.

On this basis Gollmann concludes that having to rely on trust is bad for security. Blasco Alís [33] analyses the use of generally-trusted applications such as Microsoft Excel to evade the security that is offered by Data Leakage Protection systems. For a general treatment of trust, see Gambetta et al. [119].

The term trust is used in many domains. Even when restricted to the Information and Communication Technology (ICT) domain, the meaning of the term trust is unclear. In the ICT domain trust is often based on a combination of cryptographic safeguards and procedural controls, sometimes with support from legislation. The meanings of trust and trustworthiness need to be agreed before entities such as natural persons or organisations can be considered trustworthy by other entities. However, the many different approaches taken make claims of trustworthiness difficult to compare.

In the execution of electronic transactions, there are often controls and safeguards in place, and service providers such as Trusted Third Parties (TTPs), Identity Providers (IdPs) and Trust Service Providers (TSPs) claim they can be trusted. However, what is actually meant by such trust claims is often described in vague terms, and is hard for users of the service to understand. Questions related to understanding what a specific trust claim actually means, what it is based on, as well as why it should be considered valid are hard to answer, and there is often room for multiple interpretations.

1.1.4 Ambiguity

Trust can be positive or negative. In natural language, trust is perceived as a positive term, such as trust between husband and wife, trust between business partners, and trust provided by a Trust Service Provider under the European eIDAS Regulation [103]. In the US, the National Institute of Standards and Technology (NIST) has a well-established working group called the 'trusted identities group[1]'. Here again, trust seems to be seen as positive. However, trust is

[1] `https://www.nist.gov/itl/applied-cybersecurity/tig`

also used as a negative term, in that we should try to avoid the need for trust. As noted above, Gollmann [131] states that relying on trust is bad for security.

As this ambiguity is a consequence of the widespread use of the term and the fact that English is a natural language, a rigorous framework to reason about trust, that at least clarifies some of the meanings, is a natural topic for further investigation.

The terminology related to trust also varies between European and US contexts.

- In Europe, the eIDAS Regulation [103] terminology separates identity and attribute services from signature and related services, and refers to the latter as trust services.
- In the US 'Strategy for Trusted Identities' [288], the term trust framework is used to describe the management of identities but this excludes signature and related services.

1.1.5 A lack of semantic precision

A number of initiatives have been launched with the goal of defining large-scale trust ecosystems; however they are typically not precise in their use of the terms trust and trustworthiness. Whether the meaning of the term trust in this context could be made more precise, and if so, how this could be done, are challenging research questions. The following two examples demonstrate this lack of precision.

The lack of concrete agreements on the topic of trust made by the United Nations Commission on International Trade Law (UNCITRAL) serves as a first example. UNCITRAL was established in 1966 as a subsidiary body of the UN General Assembly with the mandate to further the harmonization and unification of the laws of international trade. UNCITRAL prepared a range of conventions, model laws and other instruments dealing with the substantive law that governs trade transactions and other aspects of business law which have an impact on international trade. Trust is a recurring topic in their activities.

The UNCITRAL work is publicly available[2]. The current UNCITRAL publications do not contain a convention, model law or proposals for definitions of trust or trustworthiness. Rather they contain a series of documents that describe legal issues regarding identity management and trust services.

The second example is the absence of a definition of trust in the European eIDAS Regulation [103], enacted in 2014. The Regulation was established by the initiative of the Directorate General for Communications Networks, Content and Technology (DG Connect) of the European Commission. Article 3 of the Regulation lists a series of definitions. Trust services are defined here without defining trust itself. When consulting its authors regarding the lack of a definition of trust or trustworthiness in the legal text, they explained it is left to practitioners

[2] http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html

to agree upon the definition or meaning of trust. The Regulation is complemented by a series of implementing acts and technical standards, none of which specifically address trust or trustworthiness. The implementing acts address cross-border authentication as well as trust services such as signing, sealing, timestamping and validating. The supporting CEN and ETSI technical standards address interoperability and technical criteria at system level for PKI-based systems.

1.1.6 Lack of a precise trust definition for PKI

ETSI published a study [99] on the global acceptance of EU trust services. The report analyses trust services that operate in various regions of the world, and their possible mutual recognition and global acceptance. The study aimed to identify steps which could be taken to facilitate cross recognition between EU trust services, based on ETSI standards supporting the eIDAS Regulation, and other trust services with differing foundations. The study focussed on existing PKI-based trust services. It covers 37 PKI schemes and makes 18 recommendations. For European trust services, the main trust mechanism is the set of the EU national trusted lists. We make two observations regarding this study.

- The ETSI study covers what it refers to as the four main elements of a trust service, namely legal context, supervision and audit, technical standards, and trust representation. The study posits that trust is based on supervision and audit, together with technical standards. The meaning or semantics of trust are not addressed; the closest term that is defined is the notion of 'trust representation'. Trust representation is said to 'address the way the approval and the level of reliability of a TSP supporting given trust services is represented and disseminated; or more precisely how the confirmation that a TSP supporting given trust services meets the approval criteria applied by the supervision and auditing systems used for acceptance under the requirements of the legal context.' It is stated that such a representation can be implemented in various ways such as 'trusted lists, trust service stores, by root-signing or cross-certifying trust services, or through bridging mechanisms.'

  The trust representations that the report describes are short and focus on how trust is specified. They vary widely, and include the following:

  - UNCITRAL [318]: 'No current consensus on trust representation',
  - ISO 21188:2018 [167]: 'No requirements specified',
  - WebTrust: 'represented in the use of a licensed seal',
  - CertiPath: 'a bridge certificate',
  - SAFE-BioPharma: 'a list of cross-certified TSPs',

  - Google Chrome, Mozilla, Apple, Microsoft: 'the underlying Operating System root store'.

  In the cases of the national trust definitions for Argentina, Columbia, Switzerland and China, it was not possible to identify the chosen trust representation. Other countries such as India, Hong Kong, and Japan publish a trusted list.

- The study concludes that there remain significant issues to be overcome before global interoperability of trust services and acceptance of EU trust services can become a reality.

The descriptions of trust revealed by the study are still rather coarse. A number of recommendations are given, and the report concludes that significant issues remain to be overcome.

1.1.7 Trust and this thesis

There is no globally accepted model to describe trust in the context of digital services, nor to evaluate the trustworthiness of entities. The major contribution of the thesis is the proposal of a novel framework for assessing claims of trustworthiness, to partially fill this gap. It is based on four building blocks: a data model, rulebooks, trustworthiness evaluation functions and instance data. An implementation of this framework can be used by a potential trustor to evaluate the trustworthiness of a potential trustee.

The motivation for the work performed can be summarised as follows. The terms trust and trustworthiness are commonly used in the context of information security. However, the following observations can be made.

- As described in Section 1.1.3, there is a general lack of clarity regarding the terms.
- Section 1.1.4 pointed out that the term trust is ambiguous, as it is used for both positive and negative characterisation of entities.
- Section 1.1.5 listed some large-scale initiatives related to trust. However, they have not (yet) contributed to clearer definitions.
- As described in Section 1.1.6, PKI is the dominant security model but its semantics of trust are still rather vague.

The purpose of the work described in this thesis was to understand this better, and to investigate whether improvements could be identified. The purpose was also to investigate whether these terms could be defined more precisely, because this could lead to more effective ways of limiting interpretations and reducing inconsistency when taking trust-related decisions. This would help to better articulate what is meant by related terms such as trust model and trust policy.

1.2 Research challenges

1.2.1 Problem statement

The digital society will continue to increase its reliance on electronic transactions. Such transactions are conducted between Service Providers and Service Consumers, possibly with the use of intermediaries. The term 'trust' originates in social sciences and has been adopted by the digital society, particularly in the domain of computer security. While the notion of trust is in widespread use, interpretations of its meaning vary widely. This is a problem because it potentially leads to inconsistency.

Trust has been studied for a long time from different perspectives, including as a societal phenomenon that long predates computers. Interestingly, one could argue that the concept of trust itself is flawed; ideally, one should not 'trust' but rather take an informed decision on the basis of evidence and reasoning.

We are specifically interested in decision-making, where entities such as human or software agents want to interact with other entities. Two types of decision are of particular interest. The first is selecting which entity, service or ICT system to interact with, in cases where there is a choice. The second is whether to rely on the outcome of a transaction. We argue that it is to the benefit of potential trustors that such decisions are based on a trust model with semantics and evidence that are understandable to them.

1.2.2 Hypothesis

The following assumptions underpin the hypothesis which this thesis sets out to test.

- *Formal semantics increase trustworthiness and enable interoperability.* It is assumed that defining formal semantics for trust-related terms can be instrumental in increasing trustworthiness and in enabling interoperability across ecosystems. Such ecosystems can be organised locally or globally. Interoperability is based on mutual understanding, which requires definitions that are sufficiently precise, clear and understandable to all parties involved. Formal semantics can contribute to such definitions, and can go beyond this by also enabling automated reasoning, and providing an explanation of the outcome of such reasoning.

- *Use of information from qualified sources increases trustworthiness.* It is assumed that relevant trust-related information is provided by external information providers that have varying degrees of authority and of independence with regard to other stakeholders. Examples of such information providers include business registers, institutions that publish statements of accounts, and regulatory supervisors. These information providers make

artefacts available that offer contextual information, some of which can be used in reasoning about trust claims.

- *Linking the data from different and independent sources contributes to establishing a more complete set of information regarding a potential trustee.* This allows a trustor to rely on inputs from different sources.

On the basis of preliminary research, it was concluded that the creation of a single unifying terminology (vocabulary, ontology) to express heterogeneous trust evidence and validation is too ambitious to be addressed in a single PhD thesis. Therefore this thesis focuses on elements that can become building blocks of such a single unifying terminology.

The hypothesis underlying the work described in this thesis is as follows.

> *Where machine processable information about actors is available, it is desirable and possible to automate reasoning about the properties of these actors to support trust-related decision-making based on formal semantics.*

1.2.3 Research questions

The following research questions are addressed in this thesis with the goal of testing the above hypothesis.

1. How can trust and trustworthiness be meaningfully described in the context of the electronic society?
2. What type of reasoning could assist in automating trust claim verifications?
3. What type of information would be required to support such reasoning?
4. How can such information be harvested and transformed into a format that allows reasoning?

1.3 Research methodology

The thesis was developed according to the traditional scientific methodology (Popper [274]). A hypothesis and research questions were formulated on the basis of observations. An inductive approach was followed to propose a solution for the specific problem of how to improve interpretations of trustworthiness. The proposed solution was specified in First Order Logic. To demonstrate the practical validity of the hypothesis, a partial implementation was developed and tested. An analysis was performed of the relationship of the proposed approach to commonly accepted trust concepts. Finally, the effectiveness of the approach in meeting the

previously defined objectives was compared to that of major rival techniques, including PKIs, the Web of Trust and certain other trust-related ontologies.

1.4 Contributions

The work performed towards the PhD has resulted in the following contributions in the domain of modelling and evaluating of trustworthiness.

- A detailed literature-based review of the notions of trust and trustworthiness was performed. The review and an analysis of its findings are described in Chapter 3. The focus was on the semantics of trustworthiness and methods for the automation and interpretation of claims thereof. A classification scheme based on the formalisms and reasoning mechanisms used by the current state of the art was developed and used to identify the topics for further work.

- A novel and integrated set of requirements for trust, i.e. things which must hold for an entity to be regarded as trustworthy, is presented in Chapter 5. These requirements arise from two sources: the analysis in the structured literature review in Chapter 3, and the findings of the FutureTrust research project.

- A new approach was specified to define and evaluate trustworthiness to support the decision taking of a potential trustor regarding interacting with a potential trustee. It is referred to as the $\mathcal{TE}$ framework. It is based on the requirements developed in Chapter 5.

  The $\mathcal{TE}$ framework is a new approach for defining and evaluating trustworthiness intended to support decision-taking by a potential trustor regarding possible interactions with a potential trustee. It is designed to meet the requirements given in Chapter 5. The specification consists of the following main parts.

  - The Data Model is described as a set of predicates in First Order Logic (FOL) in Chapter 7.
  - Using the predicates defined in the Data Model, the concept of a Rulebook is given in Chapter 8. A Rulebook is a set of constraints that reflect a particular context for reasoning about trustworthiness. A Rulebook has a mandatory and a discretionary part.
    * The mandatory part contains the constraints instantiating the basic conditions for execution of the discretionary rules.

    - The discretionary part allows a trustworthiness evaluation policy to be specified by selecting those constraints that correspond to the trustor's expectations for the trustworthiness of the potential trustee.
  - Chapter 9 specifies the trustworthiness evaluation approach, which involves the following four steps:
    - choosing whether to evaluate the trustworthiness of a participant or an ecosystem;
    - selecting a particular rulebook and a set of instance data;
    - selecting discretionary constraints from the rulebook that are relevant to the trustor's decision;
    - executing the participant or ecosystem trustworthiness evaluation function to verify whether the mandatory and the selected discretionary constraints are satisfied by the selected instance data.

- A partial implementation of the $\mathcal{TE}$ framework was designed and developed to demonstrate the practical feasibility of the proposed solution.
  - The Data Model was implemented in the Description Logic OWL (see Chapter 11). It combines existing W3C ontologies with new classes and properties that were specifically created to allow semantically meaningful reasoning about trustworthiness.
  - A dedicated approach for data selection, import and transformation was implemented (see Chapter 12). The novel element is that it combines information about potential trustees from different and independent sources, using the Data Model that was implemented in OWL, in a single graph which can be queried.
  - A specific rulebook, inspired by the eIDAS Regulation [103] was implemented in the form of mandatory and discretionary constraints (see Chapter 13).
  - A trustworthiness evaluation approach was implemented using the rulebook and the data stored in the graph (see Chapter 14).

The key novel elements of the $\mathcal{TE}$ framework and its implementation can be summarised as follows.

- Information about potential trustees is obtained from multiple authoritative data sources, and combined in a graph. This is addressed as follows.
  - Requirement IR7 'Obtaining credible data' was formulated in Section 5.5.7 as follows.

As a participant in an electronic ecosystem I can understand the origin and the type of data that is used in the evaluation of trustworthiness of participants, so that I can claim the outcome of the trustworthiness evaluation is based on credible data.

  - For this purpose, the role Authentic Source was introduced in Section 6.5.1, and the attestation LegalQualification was included in the data model in Section 7.10.5.
  - The discretionary rule $\beta_{IR4\text{-}D302}$, included in Table 8.18, specifies that a participant in the role of authentic source must be attested by a legal act.
  - The selection criteria for data sources include the requirement that the data source must be authoritative for the data it provides. This is addressed in Section 12.2. Each data source that was selected for the implementation meets this requirement. An analysis of possible data sources is given in Appendices F – J. Data integration is described in Appendix L.

- Data from the selected sources was combined in a graph, using the $\mathcal{TE}$ data model that was specifically created to allow the evaluation of trustworthiness. This data model, described in Section 7.2, specifies well-defined semantics for trust and trustworthiness, and thereby improves their interpretation. This combined use of multiple authentic sources under a single data model provides an improvement over centralised hierarchical trust models.

- As the information in the selected data sources is stored in formats different from the $\mathcal{TE}$ data model, the information could not be used in its original form. Transformations from the data source formats into the $\mathcal{TE}$ data model format were created to address this issue. The information in the graph is tagged with provenance information to allow the potential trustor to trace the source of the information used in the reasoning. This provides a new way to use existing information to logically reason about trustworthiness. It is described in Section 12.2.3. Sample transformation code is provided in Appendix K.

- The formal modelling of qualifications improves the freedom of choice of the potential trustor when evaluating a potential trustee. A potential trustor can decide whether to rely on qualifications depending on the nature of the associated attestation, notably whether they are self-attested or attested by another entity. When attestations by another entity are allowed, it is also possible to specify requirements regarding the qualifications of that entity, and chains of qualifications can be modelled. A wide range of qualification types, including technical and legal qualifications, can be taken into account. The qualifications are specified in the rulebook. The concept of a rulebook is defined in Chapter 8. A specific rulebook instance, inspired by the eIDAS Regulation [103], is described in Chapter

13. The practical use of the $\mathcal{TE}$ framework for the evaluation of trustworthiness, using increasingly stringent rules, was demonstrated in Chapter 14.

1.5 Publications

1.5.1 Publications in international conferences

The following articles, closely related to the thesis, were published in the proceeding of international conferences.

- M. Sel and D. Karaklajic [298], *Internet of Trucks and Digital Tachograph Security and Privacy Threats*, Securing Business Processes – Proceedings of the ISSE 2014 Conference, Sachar Paulus, Norbert Pohlman and Helmut Reimer (editors), Vieweg+Tuebner, Springer Science+Business Media, ISBN 978-3-658-06707-6, pages 230–238. This article analyses the use of a Europe-wide PKI and trustworthy hardware to secure the digital tachograph system. This contributed to an understanding of the use of PKI and Trusted Third Parties, as formalised in Chapter 2.

- M. Sel [294], *Using the Semantic Web to generate Trust Indicators*, Securing Business Processes – Proceedings of the ISSE 2014 Conference, Sachar Paulus, Norbert Pohlman and Helmut Reimer (editors), Vieweg+Tuebner, Springer Science+Business Media, ISBN 978-3-658-06707-6, pages 106–119. This article analyses the use of classes and properties of existing semantic vocabularies (W3C, Dublin Core) to generate indicators of trustworthiness. The idea was elaborated in Chapters 7 and 11.

- M. Sel [295], *A Comparison of Trust Models*, Securing Business Processes – Proceedings of the ISSE 2015 Conference, Sachar Paulus, Norbert Pohlman and Helmut Reimer (editors), Vieweg+Tuebner, Springer Science+Business Media, ISBN 978-3-658-10933-2, pages 206–215. This article compares the EU eIDAS and US ICAM trust models. These trust models were further analysed in Chapter 2. On the basis of this article I was invited to join the FutureTrust project, to work on a trust model.

- M. Sel [296], *Improving Interpretations of Trust Claims*, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings, published in Trust Management X — 10th IFIP WG 11.11 International Conference, pages 164–173. This article proposes a preliminary approach for the evaluation of trustworthiness and the creation of a prototype in $\mathcal{SROIQ}$. This approach was elaborated in Chapter 9 and partially implemented in Chapter 14.

- O. Delos, T. Debusschere, M. De Soete, J. Dumortier, R. Genghini, H. Graux, S. Lacroix, G. Ramunno, M. Sel and P. Van Eecke, [67], *A pan-European Framework on Elec-*

tronic Identification and Trust Services for Electronic Transactions in the Internal Market, Securing Business Processes – Proceedings of the ISSE 2015 Conference, Sachar Paulus, Norbert Pohlman and Helmut Reimer (editors), Vieweg+Tuebner, Springer Science+Business Media, ISBN 978-3-658-10933-2, pages 173–195. This article discusses the pan-European framework established by eIDAS [103]. This framework was used as input to Chapter 13.

- D. Hühnlein, T. Frosch, J. Schwenk, C.-M. Piswanger, M. Sel and T. Hühnlein, T. Wich, D. Nemmert, R. Lottes, J. Somorovsky, V. Mladenov, C. Condovici, H. Leitold, S. Stalla-Bourdillon, N. Tsakalakis, J. Eichholz, F.-M. Kamm, A. Kühne, D. Wabisch, R. Dean, J. Shamah, M. Kapanadze, N. Ponte, J. Martins, R. Portela, C. Karabat, S. Stojicic, S. Nedeljkovic, V. Bouckaert, A. Defays, B. Anderson, M. Jonas, C. Hermanns, T. Schubert, D. Wegener, and A. Sazonov [161], *FutureTrust – Future Trust Services for Trustworthy Global Transactions*, Open Identity Summit 2016, 13–14 October 2016, Rome, Italy, Detlef Hühnlein, Heiko Roßnagel, Christian H. Schunck and Maurizio Talamo (editors), GI (publisher), LNI series, volume P-264, pages 27–41. This article proposes the extension of the existing European List of Trusted List towards a 'Global Trust List', and the development of an Open Source Validation Service and a Preservation Service for electronic signatures and seals. These ideas were considered in the elaboration of Chapter 9.

- M. Sel and C. Mitchell [299], *Automating the evaluation of trustworthiness*, Proceedings of TrustBUS 2021: September 2021. Springer-Verlag, 2021 (forthcoming). (Lecture Notes in Computer Science). This article summarises all key elements of the thesis.

The following article, related to trust and trustworthiness in general, was published in the proceeding of an international conference.

- M. Sel, H. Diedrich, S. Demeester and H. Stieber [297], *How smart contracts can implement 'report once'*. This article analyses the use of a blockchain and smart contracts for trustworthy reporting. A prototype, developed by the authors and implemented on a private Ethereum blockchain, is also described. The prototype was demonstrated at the Data For Policy 2017 conference, 6-7 September, London.

1.5.2 Publications from research projects

I participated in the Horizon2020 FutureTrust project[3], which ran between 2016 and 2020 and overlapped to some degree with the focus of this thesis. I was responsible for the following

[3]See `http://www.futuretrust.eu`, the project received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700542

work packages, and was lead author of the corresponding deliverables listed below.

- M. Sel, E. Üstündağ Soykan and E. Fasllija [229], *Deliverable 2.5 On Trust and Trust Models*. The concepts described in this project deliverable were used as input for Chapters 5 and 7.
- M. Sel, G. Dißauer and T. Zefferer [230], *Deliverable 2.6 Evaluation Scheme for Trustworthy Services*. The concepts described in this project deliverable were used as input for Chapters 8 and 9.

The work presented in the thesis builds on the ideas developed in these work packages. However, the work presented in the thesis is entirely my own work.

1.6 Thesis Outline

The remainder of this thesis is organised in three parts, together with a number of appendices. The main contents of the various parts of the thesis are summarised immediately below.

1.6.1 Part I Background

Part I *Background* introduces the concepts of trust and trustworthiness, and provides detailed background material built on in the remainder of the thesis. A literature survey is presented, and the logic used for formalisation of trustworthiness in Parts II and III of the thesis is introduced.

Chapter 2 on trust and trustworthiness describes the context for the key topics within the setting of Chapter 1. Introductory information sources that address topics relevant to the research questions are given. The identified topics related to trust and trustworthiness are summarised from both social and formal science perspectives, and applications of trust and trustworthiness are reviewed.

Chapter 3 provides a thorough review and analysis of the literature on trust and trustworthiness. A survey was conducted using a structured methodological approach, resulting in a shortlist of articles that are reviewed in detail. On the basis of the shortlist, an analysis was made of the state of the art on terminology related to trust and trustworthiness, as well as an evaluation of methods used for formalisation and evaluation of trustworthiness. Potential improvement points were identified.

Chapter 4 introduces the logic used to model the proposed claims and evaluations of trustworthiness. The basic notation used is described, and the implementation of $\mathcal{SROIQ}$ as OWL is discussed as this was used for the implementation.

1.6.2 Part II Modelling trustworthiness

Part II *Modelling trustworthiness* describes a new approach to the creation and interpretation of claims of trust and trustworthiness. Chapter 5 specifies requirements for describing an entity as trustworthy. Chapter 6 analyses the root causes for the problems that underlie the current state of the art and situates trustors and trustees in the $\mathcal{TE}$ ecosystem. This is a system of systems in which actors interact at their discretion. The ecosystem is structured in three planes (the enabler plane, the trustworthiness provision plane and the functional plane). The trustworthiness of entities is addressed by the $\mathcal{TE}$ framework. The next three chapters specify the main constituents of the framework.

- Chapter 7 presents the data model for the $\mathcal{TE}$ framework, which consists of a set of predicates in First Order Logic (FOL).
- Chapter 8 introduces the concept of a Rulebook, i.e. a set of constraints that reflect a particular context for reasoning about trustworthiness. Whilst the notion of a rulebook is a general one, a particular instance of a rulebook is also described which has been derived from the requirements developed in Chapter 5.
- Chapter 9 presents a formal approach to evaluating trustworthiness using the $\mathcal{TE}$ framework.

1.6.3 Part III Using trust and trustworthiness

Part III *Using trust and trustworthiness* illustrates how the approach can be applied to improve interpretations of trust claims. The practical feasibility of the $\mathcal{TE}$ framework based system is demonstrated by a partial implementation.

- Chapter 10 presents an overview of the partial implementation of the model. The implementation is described in detail in the following chapters.
- Chapter 11 presents an implementation of the data model in the Description Logic OWL. It combines existing W3C ontologies with new classes and properties that were specifically created to allow semantically meaningful reasoning about trustworthiness.
- Chapter 12 is concerned with the data import and transformation techniques that were developed to enable reasoning using data obtained from a range of sources in a variety of formats. The selection of data sources for the prototype implementation is also described, as well as the criteria that were used to select them.
- Chapter 13 describes the implementation of a specific rulebook inspired by the European eIDAS Regulation [103].

- Chapter 14 presents how the trustworthiness evaluation functions improve the interpretation of trustworthiness.
- Chapter 15 presents experimental results from the partial implementation, and a comparison with the prior art.
- Chapter 16 presents a summary of the framework and its partial implementation, the conclusions of the thesis, and ideas for future work.

1.6.4 Appendices

The following appendices can be found at the end of the thesis.

- Appendix A provides background to the literature survey that was performed.
- Appendices B and C contain the longlist and shortlist from the survey.
- Appendix D provides a short description of ontology modelling.
- Appendix E contains the description of the $\mathcal{TE}$ data model in formal notation.
- Appendices F and G provide background information on the European trusted lists and on the list of trusted lists that were implemented as a consequence of the eIDAS regulation [103].
- Appendix H describe how accreditation and conformity assessment are organised.
- Appendices I and J describe sources of company data and of natural persons used in the prototype implementation.
- Appendix K provides examples of the data transformations used in the prototype.
- Appendix L describes how the output files of the transformations were combined into a single file that can be loaded into an OWL-capable tool such as a graph database.
- Appendix M contains additional SPARQL code which demonstrates how SPARQL queries can be used to query the graph that was created as part of the prototype implementation.

Part I

Background

Chapter 2

Trust, trustworthiness and related concepts

This chapter introduces the concepts of trust and trustworthiness, together with certain related ideas. Some of the key interpretations of the terms from the social and formal sciences are introduced. This is followed by an introduction to the applications of trust in an ICT setting.

2.1 Introduction

Continuing technological advances have resulted in widespread adoption of ICT-based solutions to gain functional efficiency and monetary benefits. This adoption shows no sign of decreasing. It therefore seems reasonable to assume that the digital society will continue to increase its dependence on electronic transactions. Many such transactions are conducted between providers and consumers of services, possibly with the use of intermediaries. Relying on the outcome of a transaction performed via an ICT system, or selecting which system to use in the first place, forces the user to take a trust-related decision.

The terms trust and trustworthiness are in widespread use. This includes the common informal use of statements such as trusting one's doctor, or trusting those democratically elected not to misuse their power.

The Oxford English Dictionary defines trust as 'firm belief in the reliability, truth, or ability of someone or something; confidence or faith in a person or thing, or in an attribute of a person or thing,' and trustworthiness as 'worthy of trust or confidence; reliable, dependable.'

The close relationship between trust and dependability is illustrated by Avizienis et al. [13] who define dependability as 'The ability to deliver service that can justifiably be trusted.' Other definitions include the following.

- Castelfranchi [46] states 'trust is in fact a deficiency of control that expresses itself as a desire to progress despite the inability to control.'
- Menezes et al. [241] describe the use of a trusted third party (TTP) to overcome problems of entities that deny having signed a message or other entities falsely claiming having signed a message. In order to overcome such problems a trusted third party (TTP) or judge is required.
- The NIST framework [136] specifies trustworthiness as 'an aspect that concerns the avoidance of flaws in privacy, security, safety, resilience and reliability.'

More recently, the question has arisen whether a news item is to be trusted, or to be considered fake news. In all these situations, the meaning of these terms is not uniquely defined and differing interpretations can lead to diverging opinions.

This section provides an introduction by setting the context of this chapter. Section 2.2 discusses social science approaches to understanding and using trust and trustworthiness. This includes studies from sociological, psychological and legal points of view. Section 2.3 discusses formal science approaches. This includes a review of how logic can be applied to trust relationships followed by a computational treatment of trust. Section 2.4 discusses the application of trust and trustworthiness. This includes the relationship between trust and dependability and a discussion of distributed trust, of trust and the semantic web and of multidisciplinary approaches to trust. The chapter concludes with a summary in Section 2.5.

2.2 Social science approaches

The notions of trust and trustworthiness have been examined widely in a social sciences context. In this section we review some of the main approaches of this type to the understanding of trust.

2.2.1 Sociological perspectives

Luhmann published a seminal work, originally in two parts and in German, in 1973 (*Vertrauen*) [224] and 1975 (*Macht*) [225]. It was published in 1979 in English, as a single work, *Trust and Power* [226]. His main thesis is that trust allows the complexity of society to be reduced. Luhmann considers this complexity a problem for agents that want to align themselves with society, or adapt to it. If the complexity level is too high, it blocks adaptation. Trust allows this complexity to be reduced, and thus facilitates adaptation. As complexity increases, the need for help with adaptation also increases.

Another sociological view is presented by Barber [21], who studied the limits of trust. His view is that trust is an aspect of all social relationships. It also implies expectations about the

future based on relationships and social systems. Barber states that while *'technically competent role performance'* can be monitored (for example on the basis of results, if nothing else), an expectation regarding *'fiduciary obligations and responsibilities'* is different and more difficult. Often there exists an asymmetrical position where the trustor knows less than the trustee about such obligations. Hence the trustee must be trusted not to use this power against the trustor. The question whether trust can be transferred or generalized across relationships is also addressed. He concludes that *'It should be an axiom of social analysis that actors who perform competently or show great fiduciary responsibility in one social relationship or organization may not necessarily be trusted in others. Trust cannot necessarily be generalized.'* So a doctor's competent role performance and the meeting of fiduciary obligations may be generalizable to other patients, but not to other roles (e.g. to fix a car that has broken down). Barber thus gives three meanings to trust. One very general meaning, of trust in the moral social order, and two specific ones, technical competence and fiduciary responsibility. He also asserts that trust functions as a social control, particularly regarding the two specific meanings.

In *The evolution of cooperation* [15], Axelrod and Hamilton investigate how cooperation can emerge and persist by applying game theory. They show that even where trust is limited and the chance of communication slim, cooperation may still evolve under certain conditions. This is illustrated by the Prisoner's Dilemma from game theory. The concept was developed by Flood and Dresher and published in an internal RAND research report. Tucker [316] formalized the game and named it the Prisoner's Dilemma, presenting it as follows:

- Two members of a criminal gang are arrested and imprisoned. Each prisoner is in solitary confinement with no means of communicating with the other.
- The prosecutors lack sufficient evidence to convict the pair on the principal charge, but they have enough to convict both on a lesser charge.
- Simultaneously, the prosecutors offer each prisoner a bargain. Each prisoner is given the opportunity either to betray the other by testifying that the other committed the crime, or to cooperate with the other by remaining silent.
- The offer is:
  - If A and B each betray the other, they will both serve two years in prison;
  - If A betrays B but B remains silent, A will be set free and B will serve three years in prison (and vice versa);
  - If A and B both remain silent, they will both serve only one year in prison (on the lesser charge).

Mutual defection is the only strong Nash equilibrium in the game (i.e. the only outcome from which each player could only do worse by unilaterally changing strategy). The dilemma is that mutual cooperation yields a better outcome than mutual defection but is not the rational outcome because the choice to cooperate, from a self-interested perspective, is irrational.

The Prisoner's Dilemma game has been studied extensively, including in the 1980 tournament documented by Axelrod [14], in which a number of well-known game theorists were invited to submit strategies to be run by computers. In the tournament, programs played games against each other and themselves repeatedly. Each strategy specified whether to cooperate or defect based on the previous moves of both the strategy and its opponent. The winner of the tournament was the TIT FOR TAT strategy, which cooperates on the first move and then does whatever its opponent has done on the previous move.

Social and philosophical views of trust are combined by Gambetta. He is both the editor of the collection *Trust: Making and Breaking Cooperative Relations* [119] and author of the final chapter of this collection, *Can we trust trust?* He defines trust as follows: *'trust (or, symmetrically, distrust), is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.'* So in his view trusting a person means that the trustor takes a chance that the trustee will not behave as expected. As there is a risk involved in trusting, people tend to attempt to remove the need for trust, for example by establishing constraints. These may for example take the form of contracts, which may not be binding but are costly to fail to honour. Gambetta's paper ends with a discussion of whether or not trust is a sensible option, i.e. can we trust trust?

He also addresses the question of what could be done when either trust is so low that conditions for cooperation are not available, or when trust is not great enough to sustain potentially beneficial cooperation. It is stated that economising on trust is in general not a good strategy because it is at least as risky to fail to understand how trust works and how it relates to the conditions of cooperation. Factors such as the importance of long term arrangements, the absence of aggressive devices, the lack of ambiguity in what is cooperated about, and a step by step increase in risks involved in cooperation are seen as important. It is stated that neither trust nor potential sources of trust can be induced at will. Historical evidence is presented that it makes sense to trust trust, including a study by Vélez-Ibanez [52] of Mexican credit associations, where there is a culture construct, *confianza en confianza*. Within boundaries, trust is set high enough for tentative cooperation not to be inhibited by paralysing suspicion. It is stated that rational persons can be expected to seek evidence for their beliefs, and to offer such evidence to others. Within limits, trust can be increased or decreased by gathering information about the characteristics and past record of others. Whenever the gaps left by asymmetric infor-

mation are detrimental, they can be bridged by reputation enhancement, pre-commitment and promises. However, evidence is not seen as sufficient in its own right for trust, because trust is predicated not on evidence but on the lack of contrary evidence.

The following reasons to trust trust are put forward. If one does not trust trust, one can never find out. Trust begins with being open to evidence, acting as if one trusted, at least until more stable beliefs can be established by further information. Also, trust is not a resource that is depleted through use, instead the contrary. Trust is rather depleted by not being used. Trust can uncover dormant preferences for cooperation. If one is not prepared to trust trust, one will find that the alternatives are worse.

Bacharach and Gambetta jointly wrote Chapter 5 of *Trust in Society* [18]. They provide a theoretical framework for determining when trust and its fulfilment are to be expected. Trust is described as a particular belief which arises in games with a certain pay-off structure. They also discuss the detailed structure of the semiotics of trust. The primary problem of trust is introduced as *'Can I trust this person to do X?'* This is studied as a two-player, non-cooperative game where pay-off is determined by the players' trust, knowledge and the possibilities for rewards and punishment. The secondary problem of trust is the *'judgement of apparent signs.'* The unobservable properties of a person are called krypta. Trust-warranting properties in a trust game are called t-krypta in that game. A person's manifesta correspond to his or her observable features. A manifestum may be directly observable. Multiple manifesta might take the form of e.g. a passport. Manifesta may be evidence of krypta and t-krypta. In a game setting, the trustor needs to know the trustee, to reason about future pay-off. However, identity itself is a krypton. Because signalling theory addresses ways of signalling identity, it is important in trust problems. It can be observed that the concepts introduced in this theory are already related to authentication. They can also be linked to Sybil attacks, where the cost of establishing an identity is too low to deter an opponent from creating multiple identities as part of its attack strategy.

The increasing deployment of robots has led to research on the social interaction and trust between humans and robots. Trust as well as deception have been studied in this setting by Arkin [10].

2.2.2 Psychological perspectives

In psychology, trust relates to beliefs regarding whether the person who is trusted (the trustee) will do what is expected, as studied by Deutsch. In his foundational work 'Cooperation and trust' [69] his definition includes the term 'perceives', so it can be deduced his view on trust is a subjective one. Different agents will see beneficial or harmful outcomes differently, according to their subjective interpretations. He further elaborates the idea that cost/benefit analysis is part of taking a trust-related decision. When cooperation is considered, costs and benefits become

increasingly important. However, this raises the problem that calculating the costs and benefits for each individual outcome of a situation is time-consuming. Hence it makes sense to put limits on such calculations. Through abstraction, trust allows such limits to be implemented. It allows the trustor to treat certain things as 'given', thus avoiding the need to make calculations. In later work [70], Deutsch suggests different circumstances for trust-related choices. They include trust as social conformity, trust as virtue, and trust as confidence. The idea of trust as confidence also features in the work of various other authors, particularly Cofta [62].

2.2.3 Legal perspectives of on-line transactions

Both European and North American legislation addresses objectives related to increasing trust in on-line transactions for the benefit of dematerialisation of service provision and commerce. The scope appears similar, i.e. the primary focus is either on European cross-border transactions (both for identity and trust services), or in the US on 'interstate or foreign commerce' (with an original focus on electronic signatures, later enlarged). Mason [236] published a seminal work on electronic signatures in law. He argues that legal non-repudiation should be considered as inherently different from cryptographic non-repudiation. His article about the Single European Digital Market [237] addresses this in detail. Sel [295] provides an introduction to the trust models used in Europe and in the United States.

2.2.3.1 The European Union

European legislation is created by the European Member States, the European Commission (a source of initiatives, leading to proposals eventually implemented through programs, actions or legislation), the European Parliament (where proposals are discussed and amended, and approved/rejected) and the European Council (uniting the Ministers of the Member States). Within the European Commission, DG Connect (the Directorate General for Communications Networks, Content & Technology) took the initiative for the eIDAS regulation, covering electronic identification, authentication and trust services. The main legal document related to electronic identification and trust services is the eIDAS Regulation [103]. It is remarkable that the term trust is nowhere defined in the Regulation. There are also Implementing Decisions and Implementing Regulations for electronic identification [104, 105, 108, 109], as well as for trust services [106, 107, 110, 111]. Trust is not defined there either. Additional regulation addresses, amongst others things, reference numbers for eSignature products, Points of Single Contact and Trusted Lists. The European Commission publishes an entry point to the Trusted Lists in the form of a List of Trusted Lists. The implementation of eIDAS is technically supported by ETSI and CEN, including the development of standards.

Delos et al. [67] describes how every Member State is free to organise its trust ecosystem

within the European Union. Engelbertz [86] reviews the security of eIDAS. The FutureTrust project [161] researched the foundations of trust and trustworthiness and provided Open Source software components and trustworthy services.

Regarding identity, Member States act in a sovereign way. Each Member State organises the identity of its citizens at its discretion. Most Member States provide some form of an electronic authentication mechanism. These mechanisms include userid/password schemes, smart cards and mobile apps.

A Member State may notify one or more identity management systems to the Commission, which (after acceptance by the other Member States) leads to mutual recognition across the Member States. For this purpose, a set of minimum identity attributes has been defined [104] for natural and legal persons.

Regarding trust services, a Member State may set-up a Supervisory Body in order to monitor Trust Service Providers (TSPs), including Qualified Trust Service Providers (QTSPs). While the Supervisory Body is a Public Sector body, most TSPs and QTSPs are private enterprises. The Supervisory Body will call upon the services of a Conformity Assessment Body (CAB) to evaluate TSPs and QTSPs. Such CABs are typically private enterprises, accredited by a National Accreditation Body (NAB).

The relations between these entities can be summarised as follows. Prospective QTSPs must be audited ('conformity assessed') by a CAB. There are no prescribed standards for this purpose. However, the following applies.

- A CAB needs to be accredited by a NAB.
- A CAB must make its conformity assessment scheme public.
- The European cooperation for Accreditation[1] (EA) adopted Resolution EA 2014 (34) 22 [76] to use an eIDAS accreditation scheme based on ISO/IEC 17065 [176] supplemented by ETSI EN 319 403 [87] as one possible way for CABs to assess conformity with the relevant requirements of the eIDAS Regulation [103].

Terminology and basic definitions for electronic signatures are specified in eIDAS Article 3. Three levels of increasing reliability and protection against potential misuse are defined. For trust services, particularly electronic signatures, these are basic, advanced, and qualified. The Commission offers an anchor point from where evaluation and validation of identity and trust services can be initiated. This anchor point is legal, functional and technical. It is based on the combination of a set of legal acts and the on-line publication of signed metadata. For trust services, the List of Trusted Lists (LOTL), both in human and machine readable format, is

[1]The EA is the body recognised under Regulation 765/2008 [100] to manage a peer evaluation system across European NABs

publicly available. From this meta-data anchor point, parties such as Supervisory Bodies can be identified, and each such Supervisory Body can publish the Trusted List for its territory. Within these Trusted Lists, Trust Services Providers are identified. Qualified TSPs are subject to mandatory supervision and conformity assessment, including bi-annual audits and the use of qualified hard and software.

Regarding trust services, eIDAS Chapter III defines general provisions, the organisation of supervision, and mutual assistance amongst supervisor bodies. It defines specific requirements for TSPs and QTSPs, such as the bi-annual audit and the security breach notification requirement. Dedicated sections of eIDAS Chapter III define requirements for electronic signatures and seals, as well as electronic time stamps, electronic registered delivery services, and website authentication.

2.2.3.2 The United Kingdom

The Information Commissioner's Office (ICO) is the supervisory body for electronic trust services in the UK. According to the description on its website[2], the ICO has responsibility for supervision of the trust service provisions of the UK eIDAS Regulations. The ICO can grant and revoke qualified status for trust service providers established in the UK, approve or reject qualified trust services, report on security breaches, carry out audits and take enforcement action.

The UK legislates electronic trust services through the UK eIDAS Regulations [292]. The ICO provides guidance on this topic[3]. These UK eIDAS Regulations set out rules for UK trust services and establish a legal framework for the provision and effect thereof. They are an amended form of the EU eIDAS Regulation and retain many aspects of the EU regulation but are tailored for use within the UK. They include no provisions relating to electronic identification schemes, and exclude chapter II of the EU eIDAS regulation on this topic.

Post-Brexit, UK Statutory Instrument 2019 No. 89 [293] puts European legislation on electronic identity and trust services into UK law, and can be summarised as follows.

- Chapter II of the eIDAS Regulation [103] regarding mutual recognition and interoperability between public bodies has been revoked, including the UK implementing legislation.
- Chapter III regarding regarding mutual recognition and interoperability of trust services between EU Member States is retained and amended to preserve the regulatory framework for UK trust services. In particular, the Information Commissioner's Office (ICO) is preserved as the supervisory body for trust services in the UK. The implementing legislation that gives effect to the eIDAS Regulation [103] is revoked with the exception

[2] https://ico.org.uk/

[3] https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/

of EU 2015/1506, the Implementing Act on formats for signatures and seals [107], and EU 2016/650, Standards for the Security Assessment of Qualified Signature and Seal Creation Devices [111].

- Chapter IV is retained.

At the time of developing the implementation described in Chapter 10, the ICO was not registered in the European LOTL as TLSO.

In addition, the tScheme[4] is a not-for-profit organisation that serves organisations in the trust service provider sector. tScheme works with two recognised tScheme assessors, KPMG and LRQA, where tScheme uses the term assessor rather than conformity assessment body. Nevertheless, like conformity assessment bodies, tScheme's assessors make use of norms when performing their assessment. As a consequence it seems that the responsibilities of these assessors correspond sufficiently to those of a conformity assessment body for the purpose of the classifying them as CABs in the $\mathcal{TE}$ framework. At the time of developing the implementation described in Chapter 10, tScheme was registered in the European LOTL as TLSO.

2.2.3.3 United States

In the United States, the federal ESIGN Act [320] grants electronic signatures the same legal status as handwritten signatures throughout the United States. The ESIGN Act addresses electronic signatures as well as electronic records, both of which are commonly used in commerce today. The focus of the ESIGN Act is on interstate commerce. Due to federal preemption, the ESIGN Act allows electronic signatures when federal law applies. Where federal law does not apply, every state has an electronic signature law, most following the Uniform Electronic Transactions Act (UETA) [253].

The source of the UETA is the Uniform Law Commission (ULC) which provides law complementary to Federal US law. It is also known as the National Conference of Commissioners on Uniform State Laws. The ULC provides States with legislation that brings clarity and stability to critical areas of state statutory law. The ULC published the UETA, enacted by many states, covering retention of paper records (including cheques) and the validity of electronic signatures.

The UETA is relevant from an electronic identity and trust services perspective. It deals with enforceability of agreements and with record retention, as well as with the validation and implementation of electronic signatures and electronic records. It is limited to transactions between willing parties. The actual meaning and effect of signatures are deferred to other substantial law. However it does cover legal recognition and attribution as well as effect.

[4] urlhttps://www.tscheme.org/about-us/international-relationships

In the US public sector, a Public Key Infrastructure (PKI) is used to establish a trust infrastructure. The General Services Administration (GSA) Office of Government-wide Policy acts as the Federal Public Key Infrastructure (FPKI) Management Authority. It manages the design and development, and implements and operates the Production FPKI Trust Infrastructure. The FPKI is required for federal agencies to comply with Homeland Security Presidential Directive 12 [40] and Executive Office of the President (EOP) Office of Management and Budget (OMB) Memorandum M-11-11 [319] to accept personal identification cards and third-party credentials as directed by the OMB VanRoekel Memorandum [326].

In the US private sector, trust services such as electronic signatures are used extensively by members of the SAFE BioPharma[5] association. Also the Electronic Signature and Records Association[6] promotes the use of electronic signature and records.

2.3 Formal science approaches

In parallel, trust and trustworthiness have also been studied in the formal sciences. We review below some of the key aspects of the study of trust in this context.

2.3.1 Applying logic to trust relationships

Logic has been widely used to model trust and trustworthiness.

2.3.1.1 Logic

The Oxford English Dictionary[7] classifies logic as a branch of philosophy and defines it as follows.

> The branch of philosophy that treats of the forms of thinking in general, and more especially of inference and of scientific method. (Prof. J. Cook Wilson.) Also, since the work of Gottlob Frege (1848–1925), a formal system using symbolic techniques and mathematical methods to establish truth-values in the physical sciences, in language, and in philosophical argument.

Among the important properties that logical systems can have are consistency (no theorems contradict another), validity (proof rules do not allow a false inference from true premises), completeness (if a formula is true, it can be proven), soundness (if any formula is a theorem of the system, it is true).

[5] https://www.safe-biopharma.org/
[6] http://esignrecords.org/
[7] https://www.oed.com/

Decidability To apply logic to trust relationships requires identification of the entities for which the relationships (who to trust, who to consider trustworthy) hold. When a relationship specifies exclusion constraints[8] it is important that the entities' identities can be established in a globally unique way, because otherwise satisfaction of the constraint cannot effectively be verified. In the context of an electronic society, authentication (the confirmation that an entity is who it claims to be) is equally important.A decidable logic is required to model establishment and authentication of identity.

According to Hitzler et al. [148], a logic is decidable if there is a decision procedure for this logic. A decision procedure is a sound and complete algorithm that is guaranteed to terminate on all inputs.

- A deduction logic is sound with respect to a given semantics if every proposition set *P'* that can be derived from a set of propositions *P* by means of the deduction logic is a semantic consequence. Formally $P \vdash P'$ implies $P \models P'$.
- A deduction logic is complete if every proposition set *P'* that is semantically entailed by a proposition set *P* can also be deduced by means of the provided deduction rules; formally if $P \models P'$ implies $P \vdash P'$.

Note that the existence of a sound and complete deduction logic does not necessarily lead to a decision procedure that, given *P* and *P'*, eventually terminates and correctly answers the question whether $P \models P'$. There are arbitrarily many ways to apply the deduction rules, so in order to turn a deduction logic into a decision procedure there must also be a method determining which rules to apply and when to stop. There are logics with a sound and complete deduction calculus that are undecidable, where a logic is decidable if there exists an algorithm that will always return a correct true or false value.

Also according to Hitzler et al. [148], propositional logic is decidable, whereas in general First Order Logic (FOL) and predicate logic are not. However FOL fragments or subsets may be.

2.3.1.2 Applying logic to trust relationships

Burrows et al. [38] elaborated a logic formalism to study the authentication of principals in distributed computing systems. This formalism became known as the Burrows-Abadi-Needham (BAN) logic. They introduce semantic constructs to express concepts such as *believes, once said, has jurisdiction over* and *sees*. They make a distinction between two epochs, the past and

[8] E.g. separation of duty, which has as its primary objective to prevent fraud and errors. The objective is achieved by disseminating the tasks and associated privileges for a specific process among multiple users. This principle is demonstrated in the requirement for two signatures on a cheque.

the present, and introduce rules such as *the message meaning rule* and *the jurisdiction rule*. These are used to analyse truth and true beliefs in authentication protocols. The same authors [39] later enlarged this analysis. The BAN logic helps its users determine whether exchanged information is trustworthy, secured against eavesdropping, or both. The BAN logic was criticised [256] because it lacks a good semantics with a clear meaning in terms of knowledge and possible universes. Its critics argued that, in its idealized environment, the security of a protocol rests on two different properties. First it must distribute information to a subset of the principals. The exact nature of the predicate depends on the security protocol goals. Second the protocol must also distribute information in such a way that another subset of the population is denied access to it. In order to work properly, a security protocol must drive the state of knowledge within a distributed system so that both predicates are satisfied. The BAN logic is limited in that it only establishes predicates of the first kind. There are no postulates in the logic that deal with predicates of the second kind. This has led in the 1990s to the abandonment of BAN-family logics in favour of other proof methods. A further set of semantic constructs including *is told, possesses, once conveyed* and *believes* and rules including *being told, possession, freshness, recognisability* and *message interpretation* were introduced by Gong et al. [133].

Jøsang [188, 189, 190] proposed Subjective Logic, a calculus for subjective opinions which in turn represent probabilities affected by degrees of uncertainty. It uses a generalisation of Bayes' Theorem to enable reasoning about subjective opinions. It can be used to allow reasoning about the relative trustworthiness of information sources and the reliability of the information they provide. Jøsang [191] studied the relationship between risk and trust. Jøsang et al. [192] explored various types of trust propagation.

Küsters et al. [211] formally define accountability and its relationship to verifiability. They describe symbolic and computational accountability in terms of fairness and completeness.

2.3.2 Computational treatments of trust

Saltzer and Schroeder published a seminal paper [286] on the protection of information in computer systems in 1975. They explore the protection of computer-stored information from unauthorised use or modification. Required functions, design principles, and examples of elementary protection and authentication mechanisms are analysed. Descriptor-based protection mechanisms are elaborated, and the relation between capability systems and access control list systems are discussed. The use of segregation of duty to make ICT security solutions trustworthy was introduced in the Clark-Wilson model [60] in 1987.

Marsh [234] addresses trust from a computational perspective. A heuristic formalism is presented in Chapter 4, both in temporal and non-temporal forms, together with three types of trust, namely basic trust, general trust and situational trust. Marsh asserts that situational trust is of most importance in considering cooperative situations, such as in everyday life. Trust is

looked at from the perspective of agents, sets of agents, and societies of agents. He further distinguishes and formalises knowledge (e.g. x knows y), importance (e.g. of a to x), and utility (e.g. of a to x). Basic trust is formalised as trust of x. General trust is formalised as trust of x in y. Situational trust is formalised as trust of x in y for a. Trust is represented as a continuous variable over the range [-1, +1]. Values are calculated as weighted probabilities.

Section 8 of a report contained in Appendix C of Marsh [234] discusses the order of trust, and whether trust can be transitive. He states that trust has no ordering because it is subjective, and what one agent may call 0.5 another agent may call 0.8. As these values cannot be compared to one another, this implies that it is impossible to establish transitive relations.

The Trusted Computing Group (TCG)[9], an industry standards group, has published specifications for a Trusted Platform Module (TPM), designed to enable trust in computing platforms. TPMs have been widely deployed, and form part of the larger notion of trusted computing (see, for example, Martin [235]).

JTC 1, a joint committee of the ISO and IEC, has published the TPM specification as the multi-part standard ISO/IEC 11889:2009 [169], [170], [171], [172].

PKIs are used to establish a level of trust in the association between an identifier and a public key and/or a set of attributes. PKI trust is discussed in various Internet Engineering Task Force (IETF) Requests For Comments (RFCs), including RFC 5217 [252]. The IETF operated a working group[10] to develop Internet standards to support X.509-based PKIs. A set of provisions to organise the roles and responsibilities within a PKI are defined in IETF RFC 3647 [59].

The US National Institute of Standards and Technology (NIST) has developed [254] a description of PKI trust models and how to establish trust relations. Some widely discussed PKI trust models are illustrated in Figure 2.1, and include:

- dedicated domain CAs, where trust only applies to the certificates in the same domain,
- shared domain CAs, where certificates with the same root CA are trusted, of which a bridge CA [210] is a specific implementation,
- mutual exchange of certificates among domains and users,
- trust based on the issuing CAs listed in a trusted list.

Sel and Karaklajic [298] analysed the security and privacy threats to the Digital Tachography system. The security of the system is based on electronic authentication and electronic signatures. These are supported by a EU-wide PKI, of which the root CA is operated by the EU's Joint Research Centre in Italy, and trustworthy hardware installed in trucks.

[9]The TPM specifications are available from `https://trustedcomputinggroup.org/resources/`
[10]https://datatracker.ietf.org/wg/pkix/

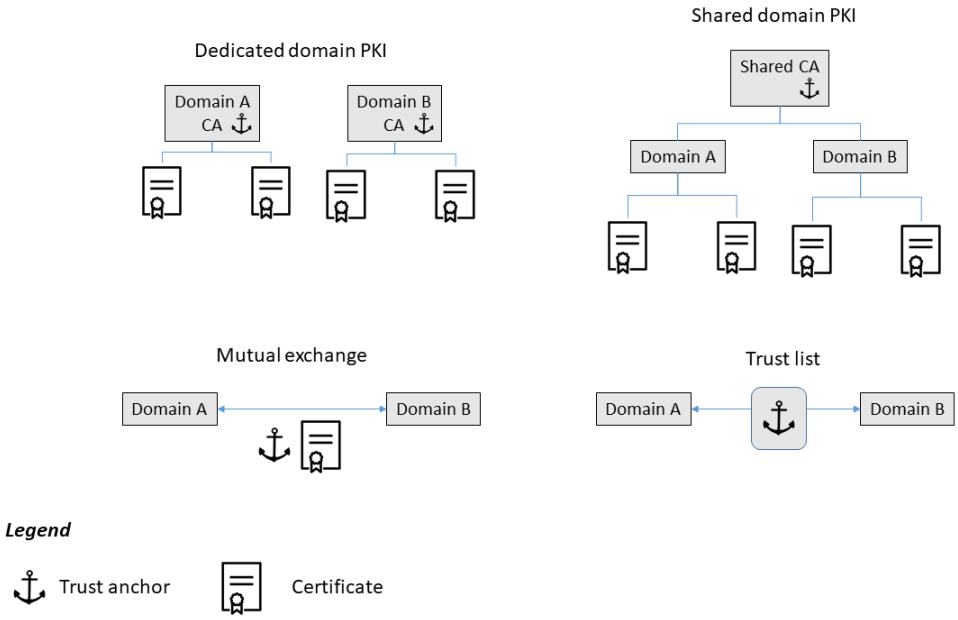

Figure 2.1: Four common PKI trust models.

Non-repudiation as provided by electronic signatures has also been studied. It typically involves an actor in the role of a Trusted Third Party, responsible for key distribution. For an introduction see Zhang [387], Coffey [61] or Onieva [265]. For an overview of how cryptography and its standards support security primitives such as non-repudiation see for example Dent and Mitchell [68].

2.4 Applications of trust

The notions of trust and trustworthiness have been applied in many settings. In this section we review some of the main uses of trust and trustworthiness in the context of ICT. An example of a multidisciplinary approach is also included.

2.4.1 Dependability and trust

A seminal article by Avizienis et al. [13] describes the relationships between dependability, security and trust. Here dependability is defined as that property of a computer system enabling reliance to be justifiably placed on the service it delivers. Depending on the application, emphasis may be put on various aspects of dependability, including:

- the property *readiness for usage* leads to availability;

- the property *continuity of service delivery* leads to reliability;
- the property *non-occurrence of catastrophic consequences on the environment* leads to safety;
- the property *non-occurrence of unauthorized disclosure* of information leads to confidentiality;
- the property *non-occurrence of improper alterations* of information leads to integrity;
- the property *aptitude to undergo repairs and evolution* leads to maintainability.

Information security is widely defined to be the maintenance of confidentiality, integrity and availability for information assets (the so-called CIA triad) -– see for example Gollmann [130]. Following Laprie [214], dependability is related to dependence and trust, and is also connected to survivability, trustworthiness and high-confidence. Five fundamental system properties can be identified: functionality, performance, dependability, security, and cost. Laprie [214] also defines a system life cycle, and a taxonomy of faults. The relationship between faults, errors and failures is described as a chain. The chain starts with either the activation of an internal dormant fault or the occurrence of an external fault. This leads to an error in a system component, which can be further propagated within the component or via a service interface into another system component. In the second system component it becomes an input error, which may propagate until it impacts a service interface, where it might lead to failure in the provision of correct service. Definitions of dependability and security are elaborated. *'The ability to deliver service that can justifiably be trusted'* is provided as the first (original) definition for dependability. *'The ability of a system to avoid service failures that are more frequent or more severe than is acceptable'* is provided as an alternate definition. Security is defined using the composite notion of confidentiality, as prevention of unauthorised disclosure, integrity, as the prevention of unauthorised amendment or deletion of information, and availability as the prevention of unauthorised withholding of information. The notions of dependence and trust are reiterated:

- The dependence of system A on system B represents the extent to which system A's dependability is (or would be) affected by that of system B.
- Trust is accepted dependence.

Accepted dependence is explained as the dependence allied to a judgement that this level of dependence is acceptable. It is stated that such a judgement might be explicit and laid down in a contract, implicit, or even unthinking or unwilling (if there is a lack of other options). It is stated that the extent to which A fails to provide means of tolerating B's failure is a measure of A's trust in B. More attributes of dependability and security are then introduced as secondary attributes.

These include robustness, as dependability with respect to external faults as well as security, accountability, authenticity and non-repudiability. It is also stated that the four concepts of dependability, high-confidence, survivability and trustworthiness are essentially equivalent in their goals and address similar threats. Means to attain dependability and security are discussed. The focus is on fault prevention, tolerance, removal and forecasting. The conclusion states that simultaneous consideration of dependability and security is relevant because in many cases a user needs an appropriate balance of their various properties. A refined dependability and security tree is presented for this purpose.

2.4.2 Distributed trust

A range of additional security and trust issues arise in the context of distributed as opposed to centralised systems.

Abbadi and Martin [1] state that the relationship between trustor and trustee in a cloud setting depends on the stakeholder type. A trustor might be interested in establishing trust in a Cloud Provider, Cloud infrastructure, and/or a Cloud user. The main properties that contribute to operational trust, namely adaptability, resilience, scalability and availability, are considered. The role of security and privacy by design for trust in the cloud is analysed. The meaning of trustworthiness is specified as 'the service performs its job as expected, which includes but not limited to considering security and privacy by design when performing any action'. The calculation of operational trust properties is discussed as a topic for further research.

Schneider and Zhou [291] consider how to implement trustworthy services using replicated state machines. They investigate the interactions of replication with threshold cryptography to achieve distributed trust. Central to maintaining system state synchronised across distributed nodes is consensus about data values. Consensus across nodes is achieved through their participation in a consensus protocol. The types of fault tolerated by the consensus protocol are an important factor. A common distinction is made between crash faults and Byzantine faults. A crash fault is a malfunction, whereas a Byzantine fault presents conflicting symptoms to different observers. The description by Lamport et al. [213] of the Byzantine generals problem in 1982 laid the foundation for Byzantine Fault Tolerance (BFT) computing. Here the difference is made between loyal generals and traitors. Acquiring consensus while tolerating Byzantine faults requires significant overhead.

When deployed within a single enterprise, or operated by a trusted authority, a crash fault-tolerant (CFT) consensus protocol might be adequate. Many such CFT protocols have been defined, including Paxos by Lamport [212]. Alternatively, in a multi-party, decentralized use case, a Byzantine fault tolerant (BFT) consensus protocol might be required. The Byzantine fault model asserts that a faulty component can exhibit arbitrarily malicious behaviour. BFT consensus has been implemented but decreases performance and throughput. The Lamport-

Shostak-Pease protocol [213] was the first BFT consensus protocol. Both CFT and BFT consensus protocols find applications in distributed ledger technologies. A distributed ledger is a ledger that is shared and synchronized, and distributed across a set of nodes. It is designed to be tamper-evident, append-only and immutable, containing confirmed transaction records. Distributed ledgers are a decentralised storage mechanism with characteristics that contribute to trustworthiness. Karame and Androulaki [196] analyse the security of blockchains.

2.4.3 Trust and the Semantic Web

The Semantic Web is a collaborative movement led by the World Wide Web Consortium (W3C). The expression 'Semantic Web' was coined by Berners-Lee [30, 301] for a web of data that can be processed by machines, where much of the meaning is machine-readable and hence can be processed automatically. Berners-Lee introduced the concept of the *Oh Yeah* browser button, by which the user can express their uncertainty about a document being displayed. The button addresses the topic of how to know information can be trusted. Upon activation of the button, the software retrieves metadata about the document, listing trust assumptions.

Semantic models are flexible and open conceptual models, examples of which include terminologies, taxonomies and ontologies.

- A terminology is a collection of terms used in a field.
- A taxonomy is a controlled vocabulary organised according to the hierarchical *(is-a)* relationships between its terms.
- An ontology is a taxonomy where each class has restrictions on its relationships to other classes or on the properties a particular class is allowed to possess. This enables consistency checking and inferencing. The root of ontologies can be found in Kripke's *Naming and Necessity* [207].

An important area of ontology research is related to the Semantic Web. The Semantic Web Stack[11] is a model for the hierarchy of technologies and languages, where each layer exploits and uses capabilities of the layers below. Trust is situated near the top of the stack[12], as illustrated in Figure 2.2.

Description Logic (DL) [281] has been widely used for ontology development and processing (see, for example Baader [16], Markus Krötzsch et al. [208]).

As DL is used in this thesis as the modelling language, an introduction is provided in Section 4.3.3.

[11] `https://www.w3.org/standards/semanticweb/`

[12] `https://en.wikipedia.org/wiki/Semantic_Web_Stack`, retrieved August 2019

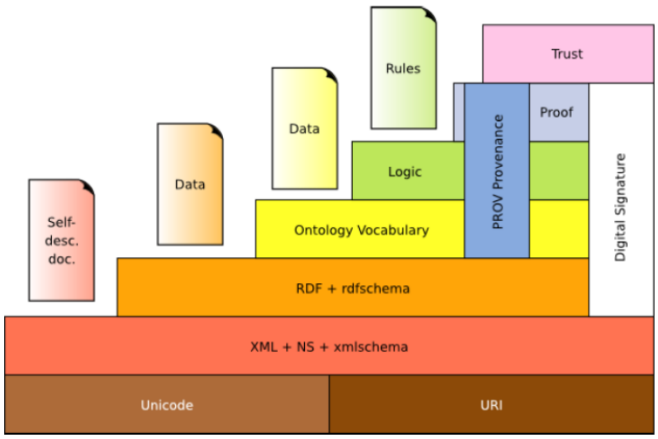

Figure 2.2: Semantic Web Stack

Viljanen [330] classified thirteen different computational trust models using nine trust decision input factors. She states there are three distinct problem areas surrounding trust, namely:

- to define the facts that support trust,
- to find the appropriate rules to derive consequences of a set of assumptions about trust, and
- how to use information about trust to take decisions.

Viljanen focuses on the first problem, although reasoning logics or negotiation protocols are not discussed. A trust taxonomy is proposed, based on nine factors. These are:

- awareness of identity,
- action (i.e. target or purpose),
- business value,
- competence (with regard to the action),
- capability,
- confidence (reflecting reputation and uncertainty),

- context,
- history (experience, evidence, local reputation), and
- third party (open trust models accept information from third parties, while closed models do not).

Van De Ven [324] studied automated legal assessment using OWL 2. An active community continues to work on legal knowledge based systems[13].

The W3C's Provenance Working Group created PROV-O, a provenance ontology[14]. Provenance plays a role in the semantic web stack's trust layer. Moreau [245] analysed how provenance contributes to trust. Ding [72] researched a provenance and trust aware inference framework in the context of US Homeland Security based on a Bayes model of belief confidence.

Lyle and Martin [227] demonstrate how Trusted Computing can be used for provenance and present an architecture for a trusted provenance system based on the hash chain mechanism implemented in a TPM. In the proposed provenance architecture, every platform is equipped with a TPM and is issued with an Attestation Identity Key, signed by a Certification Authority. Each platform will collect the information from its authenticated boot process. This information, together with each job request and result, make up the provenance data captured by the platform. This allows the provision of verifiable evidence regarding the software that was executed on the platform. The security features of the TPM contribute to guaranteeing the integrity of the provenance data.

2.4.4 Multidisciplinary approaches to trust

Cho et al. [57] provide a multidisciplinary survey on trust modelling. They address the concept of trust, its measurement, constructs and properties, as well as applications and challenges. They introduce the concept of composite trust, deriving from the interplay of unique characteristics of different layers of a network. They propose trust dimensions should be constructed in a given context, and trust should be formalised and validated according to metrics or models. These are the prerequisites for making trust assessments that can be the basis for decision-making. However, an indication of how this formalisation and validation should be done is not provided.

Mitchell [243] considers the role of trust in relationships between key parties in the 5G ecosystem and examines ways in which such trust can be provided and suggests the following.

- It is likely to be difficult for the large numbers of interacting participants in a 5G system to understand the degree to which they need to trust their suppliers, and also how they

[13] `http://jurix.nl/`
[14] `https://www.w3.org/TR/prov-o/`

might gain the degree of trust that they require.

- The absence of the appropriate levels of knowledge and trust could distort the market, and costs for all parties could be significantly higher than they need to be.
- There is a need for a framework for developing an understanding the necessary trust levels, and the way in which trust can be developed.

A potential multidisciplinary framework is introduced.

- Governmental Responsibilities: These should address the balance between governments and the market.
- Industry Organisation Responsibilities: These should address to what degree and how industry organisations should work within an industry ecosystem governance framework, and how such a framework should manage the boundaries of responsibility, power and rights of each stakeholder in the industry ecosystem.
- Technology: The question is raised whether the market can choose the most appropriate security solutions based on customer requirements, assuming governments and industry organisations are able to find ways to work together effectively to establish a system with clear boundaries of responsibility, power and rights.

2.5 Summary

Social scientists have studied trust and trustworthiness from sociological, psychological and legal points of view.

- Sociological perspectives deal with relationships between social agents and their cooperation. Trust is studied as a mechanism to reduce complexity and facilitate adaptation. The asymmetrical relation between a trustor (which typically has little information) and trustee (which typically has more information) is analysed. Game theory, when applied to trust scenarios such as the Prisoner's Dilemma, indicates that even when the conditions are such that trust is limited, cooperation may evolve. Gambetta points out that if one is not prepared to trust trust, the alternatives are worse. Together with Bacharach he studied the difference between the primary and the secondary problem of trust. The primary problem consists of finding an answer to the question *'Can I trust this person to do X?'* The secondary problem is the *'judgement of apparent signs.'* Such judgement involves signalling theory for the signalling of identity or attributes, which is particularly relevant in an electronic context where participants in transactions may not have met prior to the transaction, or may never meet at all.

- Psychological perspectives address perception and subjective interpretation. Trust is related to the belief that the trustee will do what is expected. Such a belief is subjective, as different agents will see harmful or beneficial outcomes differently, based on their subjective interpretation. Trust allows an agent's individual calculations to evaluate potential outcomes to be limited.

- The legal perspective differs in Europe and the United States.

  - In the European Union, the eIDAS regulation regulates the concepts of electronic identity, authentication and trust services. It is remarkable that, although many concepts related to trust such as trust services and trusted lists are defined, the term trust itself is not defined in the legislation. Within the European Union, Member States organise their trust ecosystem at will. Regarding identity, the main objective is to support the single market and to have recognition of electronic identity and authenticity. Regarding electronic signatures and related trust services, the objective to support the single market remains valid but additional attention is paid to implementing standards. European regulation is intended to be as technologically neutral as possible and avoids mentioning terms such as PKI in legal texts. Nevertheless PKI is the main underlying technology for authentication, signatures and the distribution of trust.
  - The United States trust ecosystem is mainly based on the federal ESIGN Act which granted electronic signatures the same legal status as handwritten signatures throughout the United States. Due to federal preemption, the ESIGN Act allows electronic signatures when federal law applies. Where federal law does not apply, every state has an electronic signature law, most following the UETA, created by the Uniform Law Commission (ULC) which provides law complementary to Federal US law. The UETA deals with enforceability of agreements and with record retention, as well as with the validating and effectuating of electronic signatures and electronic records. As in the European Union, PKI is the predominant technology in the US public sector for establishing a trust ecosystem.

In the formal sciences trust and trustworthiness have been studied from the points of view of logic and computation. Logic-based trust research focusses on a range of topics, including decision taking, decidability and interpretation. Regarding decision-taking in an electronic society, it can be observed that what Gambetta and Bacharach call the secondary problem of trust (the *'judgement of apparent signs'*) is a crucial part of the decision whether or not to engage with a participant. This decision precedes the decision whether to rely on the outcome of a transaction. Subjective Logic has been proposed as a probabilistic calculus for subjective opin-

ions. From the computational perspective, research into the protection of information systems and their security has been conducted. Protection against unauthorised use or modification has been a paramount consideration. Marsh published an influential PhD thesis addressing trust from a computational perspective. He distinguishes basic trust, general trust and situational trust. Basic trust is formalised as trust of x. General trust is formalised as trust of x in y. Situational trust is formalised as trust of x in y for a. The latter is of most importance in decisions related to cooperation.

Cryptography is a technology intimately related to security and trust. Of particular relevance here, digital signature techniques form the basis for PKI-based systems. In general, the use of cryptography gives rise to the need to distribute large numbers of keys in a secure and reliable way, which has led to the term trusted third party (TTP).

To better understand how to apply trust, the relationship between dependability, security and trust has been studied. Security has been recognised as a triad, composed of the attributes *confidentiality*, *integrity* and *availability*. Dependability is defined as that property of a computer system such that reliance can justifiably be placed on the service it delivers. Across multiple applications emphasis may be put on various facets of dependability. Dependability is analysed as a fundamental system property. Threats to dependability and security as well as the means to attain them share common elements. Dependability is defined as the ability to deliver services that can justifiably be trusted. Trust can also be seen as accepted dependence.

The Semantic Web is a collaborative movement led by the World Wide Web Consortium (W3C). The expression 'Semantic Web' refers to a web of data that can be processed by machines, where much of the meaning is machine-readable, and hence can be processed automatically. To make such processing trustworthy it is common to rely on metadata. To process both the data and the corresponding metadata, semantic models have been proposed. These are commonly classified as terminologies, taxonomies and ontologies. A terminology is a collection of terms used in a field. A taxonomy is a controlled vocabulary organised according to the hierarchical *(is-a)* relationships between its terms. An ontology is a taxonomy where each class has restrictions on its relationships to other classes or on the properties a particular class is allowed to possess. This enables consistency checking and inferencing, which is relevant to establishing trustworthiness. The W3C standardised OWL as a Web Ontology Language. There exist decidable versions of OWL, allowing the creation of ontologies that can be processed by automated reasoners in a reasonable time. Using OWL to automate legal assessment has been studied. It has been studied how provenance can be formalised in an OWL ontology, and how it contributes to trust.

Trust can also be seen from a multidisciplinary point of view, which leads to the concept of composite trust. Its components can be derived from the characteristics of the different element that are involved, e.g. the layers of a network. These characteristics can be aggregated into trust

dimensions. On this basis a composite trust model can be constructed.

The following critical observations can be made.

- While it seems reasonable to expect definitions of trust and trustworthiness to be provided, as there is an explicit trust layer in the semantic web stack (see Figure 2.2), these definitions are lacking.
- The European eIDAS Regulation [103] that specifically covers trust services does not include a definition of trust.

Chapter 3

A structured literature review

This chapter provides a detailed literature-based review of the notions of trust and trustworthiness, and an analysis of its findings.

3.1 Introduction

In this chapter we present the results of a formally structured review of the literature on trust and trustworthiness, focusing on those aspects of the greatest relevance to the main focus of this thesis. The main purposes of this review were to obtain a better understanding of the prior art, and to identify areas where further work is needed.

A particular focus was on the semantics of trustworthiness and methods for the automation and interpretation of claims thereof. The scope of the review was limited to formal models of trust and trustworthiness with a focus on semantic models.

This chapter consists of the following sections. Section 3.2 describes the methodology used to conduct the review. The protocol used and details of the realisation of the methodology are given. Section 3.3 describes the first phase of the review. It covers the preparatory steps, including the definition of the scope and purpose of the survey, and the identification of search terms and information sources. Section 3.4 covers the search over the selected information sources. The criteria for creating an initial list ('longlist') were defined and the information sources were searched using these criteria. This led to the selection of 125 articles. This selection was narrowed by defining a second set of criteria. Applying these criteria led to the creation of the final list ('shortlist') which contained 33 articles. Section 3.5 describes the analysis performed on the articles in the shortlist. This included a classification according to the formalisms and reasoning mechanisms used, which resulted in five clusters. Further research topics were identified. Section 3.6 summarises the work done.

Appendix A provides additional information on the survey. The articles included in the

longlist and shortlist are listed in Appendices B and C.

3.2 Design of the review methodology

The details of the methodology that was used to conduct the literature review are specified. This includes the specification of the protocol used and a breakdown of the work performed. A critique on the methodology is also provided.

3.2.1 Protocol

As the research domain was broad, the need to use a structured method was identified. The protocol used is a combination of those proposed by Vom Brocke [331] and Okoli [260], introduced below. As the review was carried out by the author alone, there was no need for synchronisation with other researchers. Searches were performed in the order described, using the RHUL Library Search facilities. When an article was identified during multiple searches, it is only reported in the first search. Lists of articles are ordered according to the last name of the first author.

3.2.2 Background to the approach

As noted above, the approach used for the survey is based on Vom Brocke et al. [331] as refined by Okoli [260]. Vom Brocke proposed an approach to performing a systematic literature review, formalising the need for researchers to document such searches. The Vom Brocke literature search framework consists of five phases. In the first phase, the review's scope and flavour are defined. Vom Brocke suggests basing reviews on the Cooper literature review taxonomy [64] which contains six characteristics, namely focus, goal, organisation, perspective, audience and coverage of the review. The second phase studies the key topics within the scope of the review and identifies the main relevant concepts. This helps consolidate existing information and identify areas where new knowledge may be needed. The third phase involves the actual literature search, in journals and databases of articles and proceedings. Phase four consists of analysis and synthesis, which is followed by writing up questions for future research in the fifth and final phase.

Okoli [260] further elaborated Vom Brocke's work. He refined Vom Brocke's approach to the third phase by dividing it into eight detailed steps. These are:

- Purpose of the literature review,
- Protocol and training,
- Searching for the literature,

- Practical screening,
- Quality appraisal,
- Data extraction,
- Synthesis of studies,
- Writing of the review.

These steps were used for the creation of a specific approach for the survey.

3.2.3 Approach used

3.2.3.1 Breakdown of work

Building on the schemes of Vom Brocke and Okoli, the following breakdown of work was defined.

- Preparation:
  - Specification of scope, purpose and survey questions,
  - Identification of:
    - candidate search terms,
    - candidate information sources,
  - Selection of search terms and information sources,
- Execution:
  - Search and creation of longlist,
  - Qualification of articles and creation of shortlist,
- Analysis:
  - Review of articles included in the shortlist,
  - Identification of future research topics.

3.2.3.2 Critique

The above method is not without bias, and is by no means the only one possible. A key area for possible critique is how selections are made. The above method included three selections:

- information sources,

- search terms,
- articles.

A broad set of potential information sources was surveyed, as described in Section 3.3.3. The Web Of Science Core Collection was used as a starting point. However, it is clearly impossible to guarantee completeness.

Furthermore, the choice to use search terms can be challenged. It is equally possible to search on the basis of:

- authors,
- institutions,
- journals,
- other factors, such as references, further citations, quality of abstract or introduction, quality of writing, etc.

Regarding the selection of articles, two techniques were used to try to minimise the risks of the exclusion of potentially valuable articles:

- the introduction of a longlist and a shortlist, each created on the basis of its specific longlist and shortlist selection criteria, and
- survey and review articles were considered.

However, the definition and application of the longlist and shortlist selection criteria might suffer from incompleteness, lack of depth or incorrect application. This may also apply to the survey and review articles.

3.3 Preparation

Preparation for the search involved defining the scope and purpose, specifying motivating questions, and selecting search terms and information sources.

3.3.1 Scope, purpose and questions

The scope of the review was limited to formal models of trust and trustworthiness with a focus on semantic models. Where probabilistic models overlap with this scope, they have been included.

The purpose of the review was to build an understanding of the semantics of trust and trustworthiness, as well as methods for the automation and interpretation of claims thereof. The following questions were prepared to motivate the review.

- What is today's perspective on formal and semantic models of trust and trustworthiness?
- How is trustworthiness formalised and evaluated today, how are claims interpreted?
- What are the main potential improvement points?

3.3.2 Search terms

Candidate sources such as the Web of Science[1] (WOS) suggest various ways of formulating search terms. The following are common ways of expressing a terminology and search terms for a domain:

- Unstructured, or natural language vocabularies, where there is no restriction on the vocabulary, and
- Structured vocabularies, where restrictions are imposed:
  - *Controlled vocabularies* provide a way to organize knowledge for subsequent retrieval. They are used in subject indexing schemes, subject headings, thesauri, taxonomies and other form of knowledge organization systems. Controlled vocabulary schemes mandate the use of predefined, authorised terms that have been preselected by the designer of the vocabulary, in contrast to natural language vocabularies.
  - *Taxonomies* are created according to a scientific protocol, consisting of identifying and naming species and arranging them into a classification.
  - *Ontologies* formally represent knowledge as a set of concepts within a domain, and the relationships between those concepts. An ontology can be used to reason about the entities within that domain and may be used to describe the domain.

Both structured and unstructured vocabularies were used to identify the initial search terms.

3.3.2.1 Natural language vocabulary

To identify the initial search terms using a natural language vocabulary, a combination of an English dictionary with a historical background and two modern electronic search engines was used:

- the Oxford English Dictionary[2],
- Google Scholar[3], and

[1] `https://clarivate.com/webofsciencegroup/`
[2] `https://www.oed.com/`
[3] `https://scholar.google.com/`

- Microsoft Academic[4].

The Oxford English Dictionary (OED) is an authority on the English language, providing basic descriptions of words. The OED provides a guide to the meaning and history of more than 280,000 terms. As an historical dictionary it is different from dictionaries of current English where the focus is on present-day meanings. It contains the following descriptions:

- Trust: Firm belief in the reliability, truth, or ability of someone or something; confidence or faith in a person or thing, or in an attribute of a person or thing.
- Trustworthiness: Worthy of trust or confidence; reliable, dependable.

For semantics of trust or trustworthiness, no dictionary entries were found. Hence no specific candidate search terms were identified.

The Google Scholar user interface allows querying through search terms and natural language. It uses underlying structures which are not made public. Hence it was regarded as a natural language vocabulary. The selection that Google Scholar makes is not transparent. It ranks the search results and shows only the first 1,000 results of any search, based on algorithms that Google changes at their discretion. A search for 'trust' with the period not specified returned about 3,700,000 results. Specifying the period as 2009-2019 returned about 1,690,000 results. Details can be found in Appendix A.1.1.

Microsoft Academic allows searching by author, author institution, paper publication title, journal, topic and conference. Like Google Scholar it is not transparent about the classification algorithms used for searches. Nevertheless, as the tool covers a wide range of academic sources, searches including trustworthiness were conducted. These searches returned thousands of results. Details can be found in Appendix A.1.2.

3.3.2.2 Structured vocabularies

Providers of information that make use of structured vocabularies include:

- the Web of Science[5] (WOS),
- the 2012 ACM CCS Classification[6],
- the IEEE taxonomy[7], and
- the Computer Science Ontology[8].

[4] https://academic.microsoft.com/
[5] https://clarivate.com/webofsciencegroup/
[6] https://dl.acm.org/ccs
[7] https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/ieee-taxonomy.pdf
[8] https://cso.kmi.open.ac.uk/home

Details on the analyses performed on these structured vocabularies can be found in A.1.4. Key aspects are as follows.

- The WOS makes use of keywords, and 252 subject categories mapped to 151 broadly defined research areas, including Engineering, Chemistry, Computer Science, Physics, and Mathematics. No keywords, categories or research areas are directly related to trust or trustworthiness.
- The 2012 ACM Computing Classification System (CCS) is a poly-hierarchical ontology, integrated into the search capabilities and topic displays of the ACM Digital Library[9]. A search in the on-line ACM CCS at the top level yielded four results for the term trust, and no results for the term trustworthiness.
- The IEEE publishes the IEEE Taxonomy, made up of three hierarchical levels under each term-family (or branch) formed from the top-most terms of the IEEE Thesaurus. This is a controlled vocabulary of about 10,100 descriptive engineering, technical, and scientific terms as well as IEEE-specific society terms. The taxonomy did not yield any useful search terms. No matches were found for trustworthiness. The thesaurus yielded a number of terms. Those are listed in Table A.4.
- The Computer Science Ontology (CSO) [285] is a large-scale ontology of research areas that was automatically generated using the Klink-2 algorithm [268] on the Rexplore dataset [269]. This dataset consists of about 16 million publications, mainly in the field of Computer Science. A search for 'semantics' returned 13 results, listed in Table A.5. No matching CSO concept was identified for the terms 'semantics of trust' or 'semantics of trustworthiness'.

Details on the selection of the search terms are given in Appendix A.1.3. The resulting search terms were:

- From the unstructured sources:
  - semantic trust model,
  - evaluation of trust,
  - computational trust models,
  - ontology based reasoning about trustworthiness,
  - ontologies for trustworthy solutions,
  - trustworthy fulfilment of commitments,

[9] `https://dl.acm.org/`

- trustworthiness measurement from knowledge graph,

- From the structured sources:
  - trusted computing,
  - denotational semantics,
  - argumentation semantics.

3.3.3 Information sources

3.3.3.1 Candidate information sources

The identification of candidate sources was based on discussions with my supervisor, a study of the Royal Holloway University of London's Information Security Group training material on the topic, a review of trust related and semantic web related conference proceedings (IFIP TM, DEXA/TrustBus, ISWC) and on-line research. Candidate sources were divided into two tiers. The first tier consists of providers that make citation indexing and ranking a core part of their offering. The second tier consists of providers that mostly focus on offering access to information repositories, including libraries, search engines and publishers. Details are provided in Appendix A.1.5.

3.3.3.2 Selection criteria for information sources

The following selection criteria were defined to select sources for searching. The search was designed to use both broad and deep information sources of verifiable quality. For broadness, electronic research repositories such as Web of Science, IEEE, Elsevier, and ACM were included. For depth, this was complemented by sources that are specifically dedicated to topics related to the research questions of the review.

3.3.3.3 Searches for information sources

The Web of Science Core Collection (WOS CC) was used as the initial source. The WOS indexes bibliographic records, split into citation indexes. Given the scope of the review, the Science Citation Index Expanded (SCIE) is the primary index to consider, complemented by the Emerging Sources Citation Index (ESCI). A first search of the WOS Master Journal List[10] (MJL) was conducted for the WOS Core Collection, using 'trust' as search term. The names of two journals were returned:

- Game and Wildlife Conservation Trust Review (annual), Game and Wildlife Conservation Trust, ISSN: 1758-1613,

[10] http://mjl.clarivate.com

- Journal of Trust Research[11] (semi-annual), Routledge Journals, Taylor and Francis, ISSN: 2151-5581.

The scope of the first journal did not match the review scope, and hence this was not considered. The second journal describes itself as an inter-disciplinary and cross-cultural journal dedicated to advancing cross-level, context-rich, process-oriented, and practice-relevant research. The journal addresses the fundamental nature of trust (e.g. psychological attitude and/or behavioural choice; trustfulness and/or trustworthiness), the key components of trust, and the distinction and link between cognitive (rational and instrumental), affective (emotional and sentimental), norm-related (cultural and ethical), and rule-related (market and legal) components of trust. Its scope did not match that of the review, and hence this journal was not considered further.

A second search was conducted of the WOS MJL, in the WOS Core Collection, using *trust semantic* as search term. This search returned no result.

A third search was conducted of the WOS MJL, in the WOS Core Collection, using *semantic* as search term. This search returned three journals:

- International Journal of Semantic Computing (quarterly), World Scientific Publishing Company PTE LTD, 5 Toh Tuck Link, Singapore, Singapore, 596224, ISSN: 1793-351X, index: Emerging Sources Citation Index,

- International Journal on Semantic Web and Information Systems (quarterly), IGI Global, 701 E Chocolate Avenue, STE 200, Hershey, USA, PA, 17033-1240, ISSN: 1552-6283, index: Science Citation Index Expanded,

- Semantic Web (bimonthly), IOS Press, Nieuwe Hemweg 6B, Amsterdam, Netherlands, 1013 BG, ISSN: 1570-0844, index: Science Citation Index Expanded.

The Association for Computing Machinery (ACM) publishes conference proceedings, journals, magazines, books and newsletters. They publish two journals that have trust within their scope:

- *Transactions on Cyber-Physical Systems (TCPS)*, whose scope includes Trustworthy System Designs. It is indexed by most indexing mechanisms but its most cited articles cannot be directly identified from the journal's website. Its most cited articles are, however, likely, to be included in the WOS searches.

[11] https://www.tandfonline.com/toc/rjtr20/current

- *Transactions on Economics and Computation (TEAC)*, focusing on the intersection of computer science and economics. Its scope includes computational social choice, recommendation/reputation/trust systems, and privacy. This overlapped less with the scope of the literature review.

The ACM also publishes the *Transactions on Privacy and Security (TOPS)*, previously referred to as TISSEC, but its focus does not explicitly include trust or trustworthiness.

The ACM organises a number of Special Interest Groups, with SIGSAC[12] focussing on Security, Audit and Control. There was no immediate reference identified to trust or trustworthiness in its activities or publications.

Elsevier publishes the *Journal of Web Semantics* as well as *Computers & Security*, the journal of Technical Committee 11 (Computer Security) of the International Federation for Information Processing (IFIP).

IOS publishes 95 journals, including the *Semantic Web Journal (SWJ)* and the *Journal of Computer Security (JCS)*. Both the SWJ and the JCS are indexed by most indexing mechanisms but its most cited articles cannot be directly identified from the journal's website. It is assumed their most cited articles are included in the WOS searches.

IEEE produces many publications, of which the most relevant within the search scope appear to be:

- IEEE Transactions on Dependable and Secure Computing (TDSC),
- IEEE Computer Society's Technical Committee on Security and Privacy[13]
  - Magazine on Security and Privacy,
  - Proceedings from conferences, workshops and symposia on Security and Privacy.

The publications from the IEEE Computer Society's Technical Committee on Security and Privacy (the magazines and conference proceedings) were browsed on-line (2/8/2019). It was subsequently concluded that there was little if any work published regarding the semantics of trust and trustworthiness, and hence these were not further investigated.

With Marsh as editor, SpringerOpen published a dedicated *Journal of Trust Management*[14] in the past. However, this ceased publication as of 15 June 2017.

3.3.4 Selection

Using the search terms across the information sources returned a variety of results that reflect the broad topic range. Casting results aside that were too far removed from the research

[12] https://www.acm.org/special-interest-groups/sigs/sigsac
[13] http://www.ieee-security.org/:
[14] `https://journaloftrustmanagement.springeropen.com/`

topic (wildlife conservation, psychological attitude and/or behavioural choice), the WOS MJL returned three journals that cover semantics: *International Journal of Semantic Computing* (World Scientific Publishing Company), *International Journal on Semantic Web and Information Systems* (IGI Global), and *Semantic Web* (IOS). On trust semantics the WOS MJL returned no useful results. ACM TCPS appeared to be a relevant source, but given the lack of direct searching possibilities it was assumed its articles are included in WOS searches. Elsevier and IOS have dedicated publications regarding semantics. Elsevier publishes the *Journal of Web Semantics*, while IOS publishes the *Semantic Web Journal*. The IEEE has a variety of interesting publications but these do not cover semantics.

To make sure sufficiently broad sources were included, it was decided to include the conference proceedings from the TrustBus and the IFIP TM conferences, as publications from the Journal of Trust Management often referred to articles that appeared in those proceedings. Furthermore the services from the Digital Bibliography & Library Project (DBLP)[15], Google Scholar[16] and Microsoft Academic[17] were added as these are broad sources of information.

On this basis, the following sources were selected:

- WOS,
- TrustBus and IFIP TM conference proceedings,
- Journal of Web Semantics,
- Computers & Security journal,
- Journal of Trust Management,
- DBLP,
- Google Scholar and Microsoft Academic.

3.4 Execution

The creation of an initial 'longlist' and its refinement into a focused 'shortlist' are discussed. This includes the creation of selection criteria for both lists and the execution of the search across the sources.

[15] `https://dblp.uni-trier.de/`
[16] `https://scholar.google.com/`
[17] `https://academic.microsoft.com/home`

3.4.1 Longlist criteria

The longlist was created using a screening process. Articles, including literature reviews and surveys, were included in the longlist if they appeared in the search result of at least one of the sources identified in the previous section, and either

- their title or abstract indicated they address a problem that is the same or closely related to the problem described in the thesis problem statement, defined in Section 1.2.1, or
- They address the research questions described in Section 1.2.3.

3.4.2 Performing the search

A longlist was created by searching the information sources selected in Section 3.3.4 using the search terms defined in Appendix A.1.4.2 and selecting articles on the basis of the longlist criteria defined above. This resulted in the following selection:

- WOS: 25 articles were included,
- IEEE Transactions on Dependable and Secure Computing: 5 articles were included,
- TrustBus and IFIP TM conference proceedings: 48 articles were included,
- Journal of Web Semantics: 5 articles were included,
- Computers & Security journal: 5 articles were included,
- Journal of Trust Management: 2 articles were included,
- DBLP: 16 articles were included,
- Google Scholar: 7 articles were included,
- Google Scholar and Microsoft Academic were additionally searched for surveys and literature reviews, from where 11 articles were included.

3.4.3 Longlist and shortlist

As a result of the search the longlist contained 125 articles, listed in appendix B. The articles in the longlist were screened according to their relevance. For this purpose the following shortlist criteria were adopted.

- Shortlisted articles must match the defined scope of the thesis, namely semantic and formal models of trust and trustworthiness. The focus was on models based on logic rather than on statistics, probability, social networks or reputation. Probabilistic models were excluded from the scope as they are based on statistics rather than on logic.
- They must have the potential to contribute to addressing the research questions given in Section 1.2.3.
- They must be based on sound and transparent research methodologies.

On the basis of these criteria, 33 articles were included in the shortlist, including five survey/review articles. The shortlist is provided in appendix C.

3.5 Analysis

All articles were analysed to determine whether they contribute to building an understanding of the semantics of trustworthiness and/or methods for the automation and interpretation of claims thereof, as described in Section 3.3.1. In a first step the surveys and reviews were analysed. The focus was on the identification of trends and themes, and on areas for improvement. Subsequently all remaining articles were analysed. Here the focus was on the formalisms used, both for data modelling and for reasoning. For those articles that were found to be relevant to the thesis, a short criticism was provided.

The bibliographic references in the text use the name of the author(s) for articles that have maximum two authors. When an article has more than two authors, the name of the first author is used, followed by *et al.* The full list of authors can be found in the bibliography.

In the tables the models are referred to using the name of their first author for the sake of brevity.

3.5.1 Surveys and reviews

3.5.1.1 Overview

Two surveys contain material particularly relevant to the scope and objectives of the thesis:

- The survey by Cho et al. [57] on trust modelling introduces a four-dimensional composite trust model with dimensions communication trust, information trust, social trust and cognitive trust. Cho et al. conclude that, as networks become more complex and interwoven, deriving trust becomes highly complex. For quantification of trust the identification of key trust dimensions is the first step, followed by formalising trust and validating its metrics or models. Only then can accurate trust assessments be made.

- The review by Mahmud and Usman [231] covers trust establishment and estimation in cloud services. The article starts with a background discussion of the NIST cloud model and cloud computing [239], and introduces trust management. A trust establishment and evaluation framework is presented that starts from security, privacy and SLA measures. From this 'rooted trust' is derived. There are however no goals or objectives defined hence it is hard to conclude whether the measures achieve their intended goals. A taxonomy is presented, divided into policy based trust models (in fact based on legislation rather than policy) and miscellaneous schemes, estimation frameworks, statistical and probabilistic methods, fuzzy logic, multiple criteria decision making and algorithmic solutions. The analysis covers trust factors, experiments, benefits and limitations. The term trust factor is not explicitly defined, but covers a wide range of concepts such as security, risk, privacy, auditability, scalability etc. The future research directions include trust transparency, bio-inspired methods, trust in mobile cloud, higher order statistics, and evidence-based trust.

The following three articles provided interesting background reading but did not yield relevant observations:

- Govindaraj's review [134] of trust models refers to trust management as introduced by Blaze et al. [34] and to the US NIST models of cloud deployment [221]. One section is devoted to the semantics of trust but it is rather short, referring to the different roles of trustor and trustee. The actual meaning of trust is not discussed.
- The survey by Habib et al. [139] focuses on trust and reputation (TR) systems. However interesting the survey, reputation-based systems are not in the scope of this thesis.
- The review by Kirrane et al. [202], titled *Privacy, Security and Policies: A Review of Problems and Solutions with Semantic Web Technologies*, does not address trust or trustworthiness.

3.5.1.2 Observations

From the survey and review articles, two observations relevant to the scope and objectives of the thesis were made:

- The survey by Cho et al. [57] identifies three steps to make accurate trust assessments:
  - the identification of key trust dimensions,
  - the formalisation of trust, and
  - the validation of its metrics or models.

A formalisation of these steps seems a relevant research topic.

- The review by Mahmud and Usman [231] introduces the term trust factor without explicitly defining it. It covers a wide range of concepts such as security, risk, privacy, auditability, scalability etc. A more explicit definition of the term trust factor seems a relevant research topic.

3.5.2 Articles

The shortlisted articles were analysed in terms of their main objectives, the formalism used for representation, and the reasoning mechanism. From this analysis five clusters emerged:

- Trust-related ontologies specified in OWL,
- Other trust-related ontologies,
- Models based on logic other than OWL,
- Probabilistic models, and
- Other models.

For each cluster the models' main objectives, chosen representation formalisms/semantics and reasoning approach are summarised in a table. Only the first two clusters contain work that is directly relevant to this thesis, and hence the work in these two clusters has been analysed in greater detail. In particular, a short set of open questions that have not been addressed by the prior art is derived from the analysis of the first cluster. In the case of the final three clusters, the analysis is restricted to a brief review of the data representations and reasoning methods used.

3.5.2.1 Trust-related ontologies in OWL

The first cluster included trust-related models based on OWL ontologies. These models are summarised in Table 3.1.

Discussion Bernabé et al. [26] propose SOFIC/Trust-DSS, a Decision Support System for intercloud trust and security, to allow secure interoperability in a trusted heterogeneous multidomain. It consists of SOFIC (an OWL ontology) and Trust-DSS (SWRL rules over the ontology and a quantification of assertions using Fuzzy logic).

Model	Main objectives	Representation formalism	Reasoning
Bernabé [26]	Decision Support System for intercloud trust and security, to allow secure interoperability in a trusted heterogeneous multidomain	Security Ontology For the InterCloud (SOFIC) in OWL	SWRL rules over the ontology and quantification with Fuzzy logic
Karthik [197]	Trust framework for sensor-driven pervasive environments	OWL ontology	Security rules in SWRL
Karuna [198]	Trust model for online health information systems	Taxonomy of trust factors and a User's Trust Profile Ontology (UTPO) in OWL which defines trust factors as classes, taking particularly their relation to the user into account	Recommender algorithms
Kravari [205]	Internet of Things trust management (short paper with only schematic description and implementation)	ORDAIN, general-purpose ontology for trust management, OWL, using RDF/XML	Aggregation and confidence level calculations
Oltramari [261]	Information and decision fusion as a decision support system on trust for humans	ComTrustO, a composite trust-based ontology framework fusion, modelled in OWL, using DOLCE as foundation	Information-based inference and decision fusion
Sel [296]	Trust modelling based on logic	OWL DL and existing vocabularies from W3C	Inference and SPARQL
Sullivan [307]	Definition of security requirements, metrics and trust terms	Ontology for trust-terms defined in OWL, including transparency, measurability, data, accountability, auditing, identification, responsibility, liability	Inference and queries

Table 3.1: Trust-related ontologies in OWL

- The Security Ontology For the InterCloud is the ontology on which the system is based. It is modelled in OWL 2 and builds on the mOSAIC ontology [248]. SOFIC is based on the concepts from NIST SP800-53 [255], the Cloud Security Alliance's (CSA) Clouds Control Matrix[18] and the ENISA guide to monitoring security service levels in cloud contracts [151]. The trust estimations use Semantic Web Rule Language (SWRL[19]) rules over the OWL ontology and are quantified using Fuzzy logic.

- The Trust and Security Decision Support System (Trust-DSS) calculates security expectations and trust values about others cloud services in order to determine if a Cloud Service Provider can trust another one for a given context, at a given time. Trust-DSS contains meta rules (which do not need to be customised) and regular rules (which do need to be customised to a specific assessment). An example of a meta-rule is the verification that the value of a parameter such as *SecurityAssessmentParameter* has a normalised value that is low (e.g. 0.2), or below a threshold. This parameter might e.g. represent the percentage of successful data migrations of the service provider, or a numerical value that represents a similar parameter.

The SOFIC/Trust-DSS model has the following issues.

- There is a lack of analysis regarding the evidence data that is required to operate the model. It is stated that 'The security evidences about a cloud service can be obtained directly from the observations of the behavior of the service.' While there is an analysis provided of the type of evidence required, whether this information is available or how it could be obtained is not addressed.

- The actual SOFIC ontology could not be analysed since it has not been made public. Two references were identified[20] (in the article and on the homepage of the author), but both were deactivated.

Karthik and Ananthanarayana [197] define a trust ontology in OWL that can be used by each node in a pervasive environment to define its own security rules in SWRL. The ontology's key classes are trust management process, trust establishment, trust update, subject and object nodes. The subject node trusts another node with the help of the trust management process. The object node is trusted. This trust is expressed in a value between -1 and +1, calculated on the basis of collected evidence. The SWRL security rules are mentioned but not explained or provided. An illustration of such a rule is available in pseudo code, where it can be seen that

[18] `https://cloudsecurityalliance.org/research/cloud-controls-matrix/`

[19] `https://www.w3.org/Submission/SWRL/`

[20] The article includes the url `http://reclamo.inf.um.es/sofic` as a reference to the actual ontology, and author's homepage has the url `http://selfnet.inf.um.es/sofic/`.

decisions are taken depending on whether the value of the calculated trust is above or below 0.3.

This model has the following issues.

- The actual trust model ontology could not be analysed since it has not been made public. The SWRL rules for calculating trust values have also not been published. This can be interpreted as a lack of transparency.
- The relationship between the ontology's classes and properties and the security rules is not specified.
- An explanation is not given for the meaning or semantics of the calculated trust value.
- There is a lack of analysis regarding the data required to operate the model. The model requires data to reason about. However whether this information is available or how it could be obtained is not addressed.

Karuna et al. [198] propose UTPO. Their objective is to model trust in online health information systems. They elaborate a taxonomy of trust factors and validate it through a user survey based on nine responses. On this basis they formulate an ontology in OWL for a recommender system. Given the limited number of user responses used for validation, and the specific focus on health information system recommendation, this article is not considered further in this thesis.

Kravari and Bassiliades [205] propose ORDAIN, an general-purpose ontology for trust management in the Internet of Things. It includes data and semantics about trust principles, involved parties, characteristics of entities, rating parameters, rule-based mechanisms, confidence and dishonesty in the environment. The ontology covers types of trust (communication, information, social and cognitive trust), types of control (centralized and distributed), the roles (Trusters, Trustees, Recommenders or Witnesses) and characteristics of Involved Parties, as well as information context, sources and aggregation as main classes. As it is a short paper, the description and implementation are schematic.

This model has the following issues.

- The actual trust model ontology could not be analysed since it has not been made public. The inference mechanisms and the rules used have also not been published.
- It is stated that 'involved parties can have any of the four potential roles: Truster, Trustee, Recommender and Witness'. However, no rationale is given why these roles have been selected, and why there could not be other roles.

- It is stated that 'at a specific time point they comply only with one of them. As a result, the role classes, subclasses of class Entity, are disjoined in ORDAIN.' However, an entity could at one time act as a Truster and later in another role such as Trustee, Recommender or Witness. How this is to be addressed is not covered.

Oltromari and Cho propose ComTrustO [261], a composite ontology of four layers (communication trust, information trust, social trust and cognitive trust) rather than a single unifying one. From each layer, corresponding trust can be inferred. Five common attributes are proposed for categorisation of trust attributes across trust domains. These are reliability, availability, confidentiality, integrity, and certainty.

Sub-attributes under each of these attributes can vary on the basis of the contextual features of a system. The structure of ComTrustO is based on the Descriptive Ontology for Linguistic and Cognitive Engineering (DOLCE) and is an extension of the CRATELO [262] ontology. ComTrustO uses information and decision fusion as a decision support system for trust in humans. Its focus is on information-based inference and decision fusion. Trust is modelled as a quality of the class Trustee, where trust can be represented by means of what is referred to as conceptual spaces. An automated reasoner such as Hermit [127] can be used to classify (sub)-attributes as (un)-trustworthy.

This model has the following issues.

- Although the article provides example attributes and sub-attributes corresponding to a trust type, there is little if any justification why these (sub)-attributes were selected, and how they contribute to the trust relationship between Trustee and Trustor.
- What data would be required to operate the model is not described. Whether this information is available for each of the layers, or how it could be obtained is not addressed.
- While it is explained a reasoner can be used to classify (sub)-attributes as (un)-trustworthy, it is unclear how this would be aggregated to draw conclusions from a set of attributes.

Earlier work of the author [296] proposes the Trust Claim Interpretation (TCI) model for semantic modelling of large-scale trust ecosystems. An OWL model is described where the creation of classes and properties are based on an extension of existing vocabularies (W3C, Dublin Core). These classes, together with related properties, are used to create assertions that represent information harvested from on-line information sources. This allows automated classification via a reasoner, as well as queries that support use cases from various actors. A general approach is presented, as well as results from a prototype implementation based on the European eIDAS and US FICAM trust ecosystems.

This model has the following issues.

- The justification of the creation of classes is not based on an analysis of requirements.
- The analysis regarding the nature of the data that would be required to operate the model is limited. What information would be required, whether this information is available or how it could be obtained, is only addressed at a high level.

Sullivan et al. [307] propose an OWL ontology for trust-terms to define security requirements and metrics. They claim that terms such as security and privacy, accountability and anonymity, transparency and un-observability are vital for defining security requirements but often substituted for one another in discussions. This leads to imprecise security and trust requirements and hence poorly defined metrics for evaluating system security. They propose a trust-terms ontology for defining the components of ICT security and trust. Central to their ontology is transparency, which requires both measurability and data, and implies accountability. Both accountability and anonymity relate to trust in their ontology:

- accountability enables auditing, is based on identification, and facilitates responsibility which implies liability;
- anonymity facilitates privacy.

This model has the following issues.

- They state that the 'trust-terms ontology represents an attempt at amalgamating these inputs to arrive at a preliminary high-level description of ICT trust.' However, no method is specified for arriving at a description of ICT trust.
- Much time is spent on informally comparing two ontology editors (CMapTools and Protégé) while the proposed ontology itself is only briefly discussed.
- The ontology is shown in a screenshot as a collection of 15 classes, connected via properties. Four object properties are defined that are intended as descriptive properties with varying strength. The following is stated.

  'Requires' and 'facilities' suggest binary type properties and these phrases are used for the more technical elements of the ontology. 'Implies' and 'fosters' are less specific and best describe relationships where other indefinite factors come into play.

  These definitions are broad, and they do not discuss on what basis they can be instantiated.

Candidate points for further research From the above summary and analysis we can extract the following questions for further research.

- How can we semantically define trustworthiness?

- How can we reason about trustworthiness?
- On what can reasoning to qualify an entity as trustworthy be based?
- How can we obtain information for use in supporting such reasoning about 'real world' entities?

3.5.2.2 Other trust-related ontologies

The second cluster includes ontology-based models that are specified in formalisms other than OWL. These models are summarised in Table 3.2.

Discussion Carpanini and Cerutti [44] propose an ontology of trust for situational understanding. They also propose a computational methodology for assessing the impact of trust associated with sources of information in situational understanding activities. They examine the Wakefield case, on the alleged links between vaccination and autism, and use it as a case study. They propose the SitUTrustOnto ontology, and illustrate its application to the case study. The ontology contains the classes Source (of information, blog posts, twits, scientific papers), Trust (describes the relationship between a source of information, a query, and a trust descriptor), TrustDescriptor (with a type ranging from *CompletelyReliable* to *Unreliable*), and Query (the situation that needs to be understood). Rules are defined in ORL [154], a language for expressing Horn clause rules. They show how their computational methodology supports situational understanding by drawing conclusions from defaults, as well as highlighting issues due to conflicts between sources of information that demand further investigation to be solved.

This model has the following issues.

- The model allows provision of a context but is limited to that. It qualifies sources of information as 'trusted' but whether the information itself can be 'trusted' is not addressed.
- The ontology was developed on the basis of a single case study (the Wakefield case on the alleged links between vaccination and autism). Whether and how this could be expanded to other cases is not discussed.

Ceolin et al. [51] propose an ontology for trust in web data specified in RDF[21]. This is an elaboration of an earlier ontology presented in O'Hara [199]. The model includes a belief operator that maps logical propositions to values that quantify their believed truth, e.g., by means of subjective opinions. A graphical representation of a trust ontology is presented.

[21] As RDF is used to model and implement the framework proposed in the thesis, Section 4.3.1 contains a description of it.

Model	Main objectives	Representation formalism	Reasoning
Carpanini [44]	Situational understanding, based on the Wakefield case study on alleged links between vaccination and autism	SitUTrustOnto with classes such as Source, Trust (describes relationship between a source of information, a query, and a trust descriptor), TrustDescriptor (ranging from CompletelyReliable to Unreliable) and Query	ORL rules (language for expressing Horn clauses)
Ceolin [51]	Ontology for trust in web data	Trust ontology in graphical representation, using RDF semantics (semantic interpretation is to be known by the trustor)	Belief calculation based on reputation and the concepts proposed by Jøsang
Fatemi [114]	Trust ontology for business collaboration	Extension of e^3value ontology [3] with the concept of trust. Modelling is done in Entity-Relationship diagrams.	Not discussed
Huang [155]	Trust ontology with a focus on transitivity	Fluents represented in situation calculus, distinguishing between trust in belief and trust in performance	Situation calculus
Jacobi [185]	Meta-modelling framework for trust in web data, allowing to transfer trust from known to unknown data	Trust ontologies assign trust values to data, sources, rules on the Web. Provenance ontologies capture data generation.	AIR, a declarative rule language, is proposed to implement the framework
Sherchan [303]	Modelling service trust including trust management phases	Trust ontology for semantic services in WSML	Ratings calculation (based on feedback given by consumers against a service's QoWS parameters), implemented in Java

Table 3.2: Trust-related ontologies not using OWL

This model has the following issues.

- They state that the risk of taking a 'leap of faith' when relying on third party agents or information can be reduced by sharing trust and trustworthiness values, along with their provenance. How provenance should be recorded or how it contributes to trustworthiness is not addressed.
- Trustworthiness is not modelled explicitly. They state that 'we consider an object o to be trustworthy by virtue of the fact that it is part of an RDF triple that is asserted.' The mere fact that a triple is asserted in a graph thus makes it trustworthy. This implies that only trustworthy triples will be included in the graph. How triples that are not deemed trustworthy are rejected is not discussed.
- Semantics follow the interpretation of RDF semantics, and it is stated that semantic interpretation is to be known by the trustor. It thus seems that the semantics are in fact left to the trustor, rather than specifying them.

Fatemi et al. [114] describe a trust ontology for business collaboration. They observe that existing ontologies for business collaboration model a situation in which all business actors can be trusted, which is not true in practice. To add trust to the business ontology, the e^3 value ontology [3] is extended. The e^3 model consists of a graphic part and a computational part. The graphic part is an Entity-Relationship diagram and the computational part is a spreadsheet with algorithms that can perform Net Present Value (NPV) estimations. A minimal approach is taken by providing only the extension that allows an actor to reason about trusting other actors, rather than adding all the nuances of the concept of trust. These extensions are the entities Value Object, Value Exchange and Actor. As the work is at a high level, it is difficult to analyse it further.

The Huang and Fox ontology of trust [155] aims to identify the semantics of trust, to develop a logical model of trust and to prove the transitivity of trust. The model is represented in situation calculus using fluents. A fluent is a property whose value changes when the situation does. The changing world is represented as a set of fluents. Trust and belief are defined as fluents. The model focuses on the relations among trust-related fluents, which are called state constraints. Only the case of certainty is addressed in the article, where believing will certainly lead to willingness to be vulnerable. The model distinguishes between trust in *belief* and trust in *performance*. Trust in performance is 'the trust in what a trustee performs'. Its formal semantics are defined in the form of a fluent using an entail predicate and a definition of context. Trust in belief is 'the trust placed on what the trustee believes.' Three types of trust sources are discussed: direct trust (resulting from interaction between trustor and trustee), relational trust (derived through trust propagation in social networks) and system trust (based on stable or

predictable functions of a system, such as institutional trust, membership based trust etc). They show that trust in belief is transitive in the context of social networks.

This model has the following issues.

- The model only covers the case of certainty, where believing will certainly lead to a willingness to be vulnerable. The complementary case of uncertainty seems equally important but is not addressed.
- How to obtain reliable information regarding a trustor's expectancies, particularly regarding belief is not discussed. Possible incentives for a trustor to share its true beliefs are not discussed.

Jacobi et al. [185] propose a framework for rule-based trust assessment on the semantic web. They argue that a data axis and a rule axis should be taken into account for such a framework, as well as two categories of data, content and meta-data. The framework proposes the Web Rule Language AIR and two ontologies. The first ontology is a rule ontology consisting of a set of rules which fire when a graph pattern specified in AIR is matched. The second ontology defines properties such as *isTrustedWith* (expressing a resource is trusted with respect to certain data) and *trustValue* (relating a numerical value to a resource). They claim that provenance[22] can be used to capture data generation. The provenance assertions together with meta-data and content assertions can be assessed using declarative rules.

This model has the following issues.

- They do not discuss how properties such as *isTrustedWith* and *trustValue* are established, or what role provenance plays in this.
- The property *trustValue* is given a numerical value such as the integer 75. How this should be interpreted is not discussed.

Sherchan et al. [303] define a reputation-based trust ontology for semantic services. Trust evaluation is based on feedback ratings provided by service consumers. Trust is defined as an 8-tuple: Trust[Trustee, Trustor, TimeStamp, TrustValue, EvaluationCriteria, Confidence, EvaluationPeriod, NumOfInteractions]. A Trustee is a service provider to which the Trust refers. A Trustor is the entity whose level of trust on the trustee is captured by the Trust. A TrustService provides functionalities such as trust bootstrapping, evaluation, update, composition and propagation. Types of trust include Bootstrapped Trust, Global Trust, Personalised Trust, Direct Trust, Composite Trust and Propagated Trust. TrustValue is the actual trust value such

[22] Provenance refers to the history of ownership of a valued object or information. The Oxford English Dictionary defines provenance as 'the source or origin of an object; its history and pedigree; a record of the ultimate derivation and passage of an item through its various owners.'

as '7'(numerical) or 'very trustworthy'(fuzzy). Central to the evaluation of trustworthiness are the raters (consumers willing to share their experiences) and the ratings (the feedback given).

This model has the following issues.

- The system uses trust values (DirectTrustValue, GlobalTrustValue, etc) such as '7'(numerical) or 'very trustworthy'(fuzzy). How the consistency of trust values is maintained across different raters is not addressed.
- The raters and their ratings determine the trust. Why and how raters should be motivated to act honestly, and how this can be managed or at least understood is not discussed. However this is fundamental to the trustworthiness evaluation.

Questions for further research The analysis of this cluster reinforces the observations made in the analysis in Section 3.5.2.1. It would seem, that very few authors discuss possible sources of information with which to reason.

3.5.2.3 Models based on logic other than OWL

The third cluster includes models based on logic other than OWL. The models are summarised in Table 3.3.

Review of representation and reasoning Aldini [4] describes a calculus for trust and reputation systems that models processes. The semantics are based on labelled transition systems. A trust label transition system *tlts* is defined as (set of states, initial state, labels, state transitions, trust predicates, labelling function). State formulae allow modelling of trust predicates.

Ferdous et al. [116] propose a model for trust issues in federated identity management. Trust is modelled between entities such as users, service providers and identity providers in federations. A distinction is made between direct and indirect trust, and a set of trust scopes is defined. Trust strength is defined as subjective trust (low, medium, high), level of assurance and federation trust (untrusted, semi-trusted, restricted-trusted and fully-trusted). Trust is then modelled in proof rules, both in dynamic and static federations.

Henderson et al. [146] describe an approach to modelling trust structures for PKI, they use predicate logic to represent a range of PKI topologies, including mesh PKIs, hierarchical PKIs and PKI bridges. Their model is designed to describe how trust is referenced within a public key. A trust anchor is any Certification Authority (or rather their certificate or public key) which is trusted without the trust being referenced through the PKI certificates. Users keep a set of

Model	Main objectives	Representation formalism	Reasoning
Aldini [4]	Calculus for trust and reputation systems	A trust label transition system *tlts* is defined as (set of states, initial state, labels, state transitions, trust predicates, labelling function). State formulae allow to model trust predicates.	Trust Temporal Logic defines conditions on actions and requirements for labelling the states. Trust function *tf* returns a yes/no answer, using a trust and a recommendation table as well as a trust threshold and a trust variation function.
Ferdous [116]	Model trust issues in federated identity management	Sets of users, service providers and identity providers, values for strength and level of assurance, actions $\rightsquigarrow$ performed via communication channels	Proof rules for dynamic and static federations, quantification by multiplication of the values
Henderson [146]	Model PKI trust structures	Uses first order logic, sets, functions to model entities, certificates, data fields	Rules with $\exists$ and $\forall$ qualifiers to verify constraint satisfaction and certificate paths calculation
Liu [220]	Modelling Certificate Management Systems	The topology structure and states of a CMS as well as a general CMS security policy are formalised in axioms.	Formal descriptions of certificate issuing, revocation and rekeying are provided as transitions that change states of the CMS. Predicate logic models the state transitions.

Table 3.3: Models based on logic other than OWL

trusted public keys of users and trust anchors. Trust is not precisely described, but a trusted certificate is 'one that is used in verification'.

Liu et al. [220] describe how to formally model trust structures for PKI and Certificate Management Systems (CMSs) using predicates and a state-based model. The topology and states of a CMS are formalised in axioms, as is a general CMS security policy. Formal descriptions for the main CMS functions, including certificate issuing, revocation and rekeying, are formalised in predicate logic as transitions that change states of the CMS. For example, a CMS policy can contain predicates such as *Trusts*(*X*,*C*). This means that if *X* trusts the certificate *C*, the predicate *Trusts*(*X*,*C*) holds. Inference rules for verification of certificates are presented, based on the predicates. However, what the predicate *Trusts*(*X*,*C*) means that is not defined, except that (as for Henderson et al. [146]) a trusted certificate is one that is used in verification.

Observations The semantics of trust in a PKI have not been defined in the work reviewed. Given that PKI has been studied extensively for several decades, this suggests that defining trust in this domain is non-trivial.

3.5.2.4 Probabilistic models

The fourth cluster includes probabilistic models. The models are summarised in Table 3.4.

Review of representation and reasoning Alexopoulos et al. [5] define M-STAR, an evidence-based software trustworthiness framework. Trust is defined as an estimate by the trustor of the inherent quality of the trustee, i.e. the quality to act beneficially or at least non-detrimentally to the relying party. This estimate is based on evidence about the trustee's behaviour in the past, in this case past vulnerabilities and characteristics of software.

Cho and Chen [58] propose PROVEST (PROVEnance-baSed Trust model) to achieve accurate peer-to-peer trust assessment and to maximise the delivery of correct messages received by destination nodes while minimizing message delay and communication cost. A node's trust is estimated in response to changes in the environmental and node conditions. Trust is quantified as a real number in the range [0,1], and trust evidence, either direct or indirect, is modelled by the Beta distribution [164]. Trust in a node is assessed in three dimensions: availability, integrity and competence (remaining battery lifetime and cooperativeness).

The trust management framework by Fan and Perros [112] covers objective and subjective trustworthiness. Central to the framework are Trust Service Providers (TSPs), mediation agents between users and providers of cloud services that are independently maintained and

Model	Main objectives	Representation formalism	Reasoning
Alexopoulos [5]	Software trustworthiness	Probabilistic, based on Bayesian statistics (CertainTrust)	CertainLogic operators, implemented in Python
Cho [58]	Peer-to-peer trust assessment to maximise message delivery while minimizing cost in networks	Probabilistic, based on Bayesian statistics (CertainTrust), trust is scaled as a real number	CertainLogic operators, implemented in Python
Fan [112]	Trust management framework for multi-cloud environments based on Trust Service Providers (TSPs)	Combination of local objective, local subjective, global objective and global subjective trust models.	Based on Josang's scalars of belief, disbelief and uncertainty
Habib [140]	Security quantification for cloud systems	Information is based on cloud providers' self-assessments through questionnaires	The level of security capabilities is quantified using CertainLogic [276]
Huang [157]	Calculus for trust and identity, structured into performance and belief trust	*trust_p(d, e, x, k)* $\equiv$ *madeBy(x, e, k)* $\Rightarrow$ *believe(d, k* $\Rightarrow$ *x)* *trust_b(d, e, x, k)* $\equiv$ *believe(e, k* $\Rightarrow$ *x)* $\Rightarrow$ *believe(d, k* $\Rightarrow$ *x)*	Proof rules and probabilistic calculation of trust aggregation and degree.
Jøsang [188] [189] [190]	Probability and uncertainty	Subjective Logic calculus for opinions which represent probabilities affected by degrees of uncertainty.	A logic for reasoning about relative trustworthiness of information sources and the reliability of their information
Ries [277] [276]	Expressing opinions	CertainTrust for representation of evidence-based trust and uncertain probabilities.	CertainLogic, a probabilistic approach based on propositional logic
Shekarpour [302]	Trust calculations and trust rating	Trust model for evaluating trust rating between two nodes as trustor and trustee (social relationship based)	An algorithm for propagation (based on statistical techniques) and one for aggregation (Fuzzy Logic)

Table 3.4: Probabilistic models for trust and trustworthiness

operated. They derive trust from monitoring. A combination of four trust models (local objective/subjective and global objective/subjective) is proposed together with a network of TSPs for trust sharing. Trustworthiness is expressed in terms of objective trustworthiness (Quality of Service, security, privacy protection and service parameters) and subjective trustworthiness (user perception and belief). A TSP derives a Cloud Service Provider's objective trust from the trust information received from monitoring agents. Subjective trust is derived by collecting trust feedback ratings sent by Cloud Service Users for services they have used. Evaluation is structured in an objective and a subjective layer.

Habib et al. propose methods to quantify the level of security capabilities in [140], using CertainLogic operators [276]. The security capability information can be based on self-assessments. CertainLogic is used to quantify the security capabilities. To facilitate human interpretation, approaches to visually communicate security capabilities are presented.

Huang and Nicol [157] propose a trust calculus for PKI and identity management, defining semantics of trust and distrust. Trust reasoning is defined for trust in *belief* and *performance*. Trust in performance is expressed as $trust\_p(d, e, x, k) \equiv madeBy(x, e, k) \Rightarrow believe(d, k \Rightarrow x)$. Trust in belief is expressed as $trust\_b(d, e, x, k) \equiv believe(e, k \Rightarrow x) \Rightarrow believe(d, k \Rightarrow x)$. The uncertainty of trust is expressed in a measurable 'trust degree', based on probability. Trust propagation in networks modelled as directed acyclic graphs can be calculated on the basis of the degree of trust. Applications to certificate chains, hierarchical and mesh PKIs are proposed, and it is shown how to calculate trust in belief and trust in performance values in the range [-1, +1]. These calculations are based on sequence and parallel aggregations of nodes in a network and probabilities.

Jøsang et al. propose Subjective Logic [190], a probabilistic logic where arguments contain degrees of uncertainty and where belief ownership is explicitly expressed. It uses a generalisation of Bayes' theorem to make it applicable to subjective opinions. It is used for modelling and analysing situations characterised by uncertainty and incomplete knowledge, e.g. for modelling trust networks and Bayesian networks. Subjective logic has also been used for legal reasoning [189].

Ries and Heinemann [277] propose CertainTrust, a model for expressing opinions that handles probabilities subject to uncertainty. CertainTrust refers to an opinion oA as the truth of a proposition A, given as oA = *(average_rating, certainty, initial_expectation_value)* where the rating and certainty are in the interval [0, 1], and the initial expectation value in (0,1). They further state that the average_rating indicates the degree to which past observations support the truth of the proposition. The certainty indicates the degree to which the average rating is assumed to be representative for the future. The initial expectation expresses the assumption about the truth of a proposition in the absence of evidence.

Ries et al. [276] propose CertainLogic, building on the concepts of CertainTrust. In Cer-

tainLogic, operators of propositional logic are defined compliant with the evaluation of propositional logic terms in a probabilistic approach. When combining opinions, the operators take care of the (un)certainty assigned to its input parameters, and reflect this (un)certainty in the result.

Shekarpour and Katebi [302] propose algorithms for propagation and aggregation of trust. They analyse four well-known methods for modelling and evaluation of the semantic web, namely the centralised model, the distributed model, the global model and the local model. Trust calculation and rating methods are categorised based on experimental results. A method for evaluating trust is proposed, associated with algorithms for propagation and aggregation. The propagation algorithm utilises statistical techniques while the aggregation algorithm is based on a weighting mechanism. The efficiency and effectiveness of the proposed method are illustrated by experimental results.

Observations The models in this cluster are probabilistic and do not primarily focus on the semantics of trust. In addition, approaches relying on quantification can be criticised for being unrealistic because there is no way to make the calculated values comparable. For example, does a value of zero indicate untrust (ignorance) or distrust (lack of trust)?

3.5.2.5 Other models

The fifth cluster includes models that do not fit any of the preceding categories. The models of the fifth cluster are summarised in Table 3.5.

Review of representation and reasoning Balduccini et al. [19] propose an ontology-based reasoning approach about the trustworthiness of cyber-physical systems. The paper enriches the model from the US National Institute of Standards and Technology (NIST) framework [136] by applying ontological approaches and reasoning techniques using the rule-based language *Answer Set Programming (ASP)* [233]. The Aspect Trustworthiness deals with the avoidance of flaws in Privacy, Security, Safety, Resilience and Reliability.

Huang and Nicol [156] state that the major PKI specification documents do not precisely define what trust exactly means in PKIs. Instead they rely on implicit trust assumptions, some of which may not be always true. These implicit trust assumptions may give rise to differences in understanding regarding the meaning of certificates and trust, which may possibly cause a misuse of trust. They argue that trust in PKI serves the logic of certification path validation, as defined in IETF RFC 5280 [63]. For certificates, three semantics are defined, followed by

Model	Main objectives	Representation formalism	Reasoning
Balduccini [19]	Requirements for trustworthiness of cyber-physical systems	Forest of concerns where trees represents aspects. Two types of nodes (concern elements and property nodes), and two types of edges (decomposition of concerns and connectors of concerns to properties)	Ontology-based reasoning, Answer Set Programming (ASP)
Huang [156]	Distinguish between implicit and explict trust in PKI	Semantics for certificates, for PKI trust and for cross-domain PKI architecture, in natural language, starting from trust in performance and in belief	Not specified, reference to the logic of certificate path validation as per RFC 5280 [63]
Li [215]	Internet of Things decentralised trustworthy context and QoS-aware service discovery framework	QoS ontology based on the W3C QoS requirements guidelines for web services with addition of one special context to model social relationships between IoT devices	Decentralized trust propagation and service discovery mechanisms are designed for service discovery, based on social recommendations
Oltramari [263]	Automated annotation of privacy policies	PrivOnto ontology in OWL	Inference and SPARQL
Ming Qu [275]	Trusted Ontology model for evaluating semantic web services	Ontology schema containing a semantic description of semantic web services	Axiom-based reasoning rules to represent and evaluate trustworthiness
Zhu [392]	Trust requirements modelling and analysis of web services	Trust ontology, based on social beliefs, formalised in Natural Language	Rules in the form of predicates plus a reputation score algorithm

Table 3.5: Other models

another for trust in a PKI system. Two more semantics are defined for cross-domain architectures. Trust in Certification Authorities is studied, and they conclude that some of the defined semantics are lacking in commonly used IETF PKI specifications, and others are only implicitly present in the specifications of certificate path validation.

Li et al. [215] propose an Quality of Service (QoS) ontology based on the W3C QoS requirements for web services, with the addition of a special context to model social relationships between Internet of Things (IoT) devices. Mechanisms for decentralized trust propagation and service discovery based on social recommendations are designed.

Oltramari et al. [263] propose PrivOnto, a semantic framework to represent annotated privacy policies. The taxonomy of Heurix et al. [147] for privacy enhancing technologies is used to structure the discussion on techniques. PrivOnto has been used to analyse a corpus of over 23,000 annotated data practices, extracted from 115 privacy policies of US-based companies. A set of 57 SPARQL queries has been defined to extract information from the PrivOnto knowledge base, to answer privacy-related questions.

Qu et al. [275] present the Trusted Ontology (TO) schema, intended to address the lack of a semantic description for information about the trustworthiness of Semantic Web Services. A Trusted Domain is divided into a Trustworthy Object Domain and a Trust Subject Domain. A series of subject and object types are defined. The TO ontology is defined as a set of six collections including domain concepts, concept attributes, and relationships and hierarchies among these concepts. Axioms, reasoning rules and a process to evaluate the trustworthiness of a Semantic Web Service are described.

Zhu and Jin [392] present a formalism for modelling trust requirements and analysing web services, using a trust ontology. The model adopts a social view of trust which includes beliefs that a trustor has on a trustee. Natural language is used rather than a formalism such as OWL. Constraints are defined in the form of rules for the various types of belief. An algorithm that computes a reputation score is proposed, to support the reputation belief.

3.5.3 Research topics

On the basis of the above analysis the following questions for further research were identified.

- How can we semantically define trustworthiness?
- How can we reason about trustworthiness?
- On what can reasoning to qualify an entity as trustworthy be based?
- How can we obtain information for use in supporting such reasoning about ‘real world’ entities?

These four questions are explored further below.

3.5.3.1 Improving the semantic definition of trustworthiness

Many of the reviewed models offer, or work towards offering, a semantic definition of trust. The main problems that can be identified are as follows.

- Most models are limited to a specific context or problem. No model is widely applicable or flexible enough to cover multiple problems.
- While PKI has been deployed at large scale since the 1980s, and the term Trusted Third Party is in common use, it is not clear what 'trusted' actually means. Huang et al. [156] state that the major PKI specification documents do not precisely define what trust means in a PKI, and there are implicit trust assumptions, some of which may not be always true. These implicit assumptions may give rise to differences in understanding regarding the meaning of certificates and trust, which could lead to a misuse of trust.

Also, as outlined in Section 1.1.2, the lack of consensus regarding whether trust is desirable in the first place contributes to ambiguity and lack of clarity. Where the distinction between trust and trustworthiness is made, there is consensus that trustworthiness is desirable. Hence it seems logical to focus on trustworthiness rather than on trust.

No model for the semantics of trustworthiness was identified that works in multiple contexts. As a consequence the improvement of the semantic definition of trustworthiness appears to be an important topic for further research

3.5.3.2 Reasoning about trustworthiness

A number of authors have devised ways to express trustworthiness as a numerical value — see, for example, Marsh [234], Jacobi et al. [185] and Sherchan et al. [303].

However, it is hard if not impossible to define semantics for numbers, and ratings or reputations of trustworthiness are subjective (what one person rates as 0.7 might be rated differently by another person). As a consequence performing calculations using numerical ratings is problematic, as is using them to model transitivity. This therefore suggests that symbolic logic is more appropriate for reasoning about trustworthiness than using a calculus based on numerical values. Devising an appropriate formalism to enable reasoning about trustworthiness is therefore a second important topic for further research. As can be seen from Tables 3.1, and 3.2 Description Logics such as OWL seem particularly relevant.

3.5.3.3 Possible bases for regarding an entity as trustworthy

Given a method to reason about trustworthiness, criteria are needed to enable a decision to be made regarding whether an entity is trustworthy (or at least sufficiently trustworthy for the

particular context). Mahmud and Usman [231] introduce trust factors. However these trust factors such as 'security' are only broadly defined, and neither is it specified precisely why and how they contribute to trust or trustworthiness. Thus a third important topic for further research involves identifying criteria regarding whether an entity is trustworthy

3.5.3.4 Obtaining information for use in reasoning

Assuming appropriate mechanisms can be defined to reason about trustworthiness and it is possible to qualify an entity as trustworthy based on such reasoning, then such mechanisms will require information about the entities to use as input. Reasoning about 'real world' entities will require a range of information sources and information types. As a consequence, the selection of information sources and information types is a fourth key topic for further research.

3.6 Summary

This chapter describes the process used, and the results of, a formal review of the relevant literature on trust and trustworthiness. The focus was on the semantics of trustworthiness and methods for the automation and interpretation of claims thereof. The scope was limited to formal models of trust and trustworthiness with a focus on semantic models. The following survey questions were put forward.

- What is today's perspective on formal and semantic models of trust and trustworthiness?
- How is trustworthiness formalised and evaluated today, and how are claims interpreted?
- What are the main potential improvements points?

The survey methodology was constructed on the basis of the structure proposed by Vom Brocke et al. [331] as refined by Okoli [260]. The survey was performed in three phases: preparation, execution and analysis.

The preparatory phase included defining the scope and purpose of the survey, and the selection of search terms and information sources. Performing the survey involved the following steps. First the criteria for creating an initial list ('longlist') were defined. The information sources were then searched using these criteria, which led to the selection of 125 articles. This selection was narrowed by defining a second set of criteria. Applying these criteria led to the creation of the final list ('shortlist') which contained 33 articles. In the analysis phase the models described in the selected articles were classified into five clusters:

- Trust-related ontologies in OWL,

- Trust-related ontologies other than specified in OWL,
- Models based on logic other than OWL,
- Probabilistic models, and
- Other models.

Ther formalisms and reasoning introduced in the various papers were analysed. For the first two clusters, a short criticism was also provided. On the basis of the above analysis the following questions for further research were identified.

- How can we semantically define trustworthiness?
- How can we reason about trustworthiness?
- On what can reasoning to qualify an entity as trustworthy be based?
- How can we obtain information for use in supporting such reasoning about 'real world' entities?

Chapter 4

Logic and the Semantic Web

This chapter introduces the logic used to model claims and evaluations of trustworthiness. The basic notation used is described, followed by a short discussion of first-order logic. Subsequently, Description Logics are introduced, and $\mathcal{SROIQ}$ is described. The implementation of $\mathcal{SROIQ}$ as OWL is discussed, as this will be used later as the particular Description Logic for the formalisation of trust claims.

4.1 Introduction

In this chapter we present the logical foundation for the framework that forms the core of this thesis, which is designed to capture claims and evaluations of trustworthiness. The framework, introduced in Chapter 6, is described in the Web Ontology Language (OWL). OWL is based on the $\mathcal{SROIQ}$ Description Logic (DL). DLs are a type of first-order logic, building on set theory.

To help ensure the use of a consistent notation for the framework, the basic terminology of sets and logic are introduced and the essential characteristics of first-order logic are discussed. As the detailed specification and implementation of the framework have been performed using semantic web software whose OWL capabilities are based on the Resource Description Framework (RDF), this framework is also described. DLs and how they can be used for knowledge representation are discussed, as these are the formalisms for our model.

This chapter consists of the following sections. Section 4.2 introduces the notation for sets and logic used to formalise the proposed model for claims and evaluations of trustworthiness. This is followed by a short discussion of first-order logic, including its syntax and semantics. Section 4.3 describes the semantic web formalisms that are used in the proposed model. It covers RDF and DLs with a focus on $\mathcal{SROIQ}$, the particular Description Logic that will be used later for the formalisation of trust claims. OWL is introduced and the correspondence

between $\mathcal{SROIQ}$ and OWL is discussed. Section 4.4 summarises the chapter.

4.2 Formal logic

4.2.1 Sets and logic — basic terminology

4.2.1.1 Sets

The terminology defined by Hitzler et al. [148] is used. Braces { } delimit the members of a set, where $\{p1, p2\}$ represents a set containing the propositions *p1* and *p2*, $\in$ denotes 'is an element of' and $\subseteq$ indicates a subset. $\top$ and $\bot$ represent true and false.

4.2.1.2 Propositional logic

Propositions are statements which can be true or false. Propositional logic[1] is a branch of logic that deals with propositions and argument flow. The symbol $\neg$ means negation. If P is a proposition, then $\neg P$ is also. The symbol $\wedge$ means logical 'and'. The symbol $\vee$ means logical 'or'.

Compound propositions are formed by connecting propositions using logical connectives. The connective symbol $:=$ corresponds to assignment. Propositions without logical connectives are called atomic propositions. Given a specific logic $\mathcal{L}$, the set of all its propositions is denoted by $\mathbb{P}$.

Argument flow makes use of sequents, consisting of premises that allow the deduction of a conclusion. Sequents are represented as *premises* $\vdash$ *conclusion*. $\mathcal{A} \vdash \mathcal{B}$ indicates that $\mathcal{B}$ can be syntactically derived from $\mathcal{A}$. The forward arrow $\rightarrow$ represents the implication connective, which is also known as material conditional, material implication, material consequence, or simply implication, implies, or conditional. It is used to form statements of the form $p \rightarrow q$ which is read as 'if p then q'. Such statements are termed conditional statements. In terms of semantics, the statement $p \rightarrow q$ means 'if p is true then q is also true', such that it is false only when p is true and q is false. The conditional statement $p \rightarrow q$ does not conventionally specify a causal relationship between p and q, and 'p is the cause and q is the consequence from it' is not a generally valid interpretation.

The symbol $\equiv$ represents equivalence, and $\Vdash$ represents the satisfaction relation.

An *axiom* is a statement that is taken to be true, to serve as a premise or starting point for further reasoning and arguments. A *model* is a mathematical structure that satisfies axioms.

A logical system is said to have the soundness property if and only if every formula that can be proved in the system is logically valid with respect to the semantics of the system. A system

[1] Propositional logic is also known as propositional calculus, statement logic, sentential logic or zeroth-order logic.

is called complete with respect to a particular property if every formula having the property can be derived using that system, i.e. is one of its theorems. The term 'complete' is also used without qualification, with differing meanings depending on the context, mostly referring to the property of semantic validity. Intuitively, a system is called complete in this particular sense if it can derive every formula that is true.

The symbol $\vDash$ denotes the models or entails relation for logics. It is used to indicate a conclusion that follows semantically from a premise. $\{p1, p2\} \vDash \{p3, p4\}$ represents the entailment of a second set of propositions by a first set of propositions. A logic $\mathcal{L}$ is composed of a set of propositions together with an entailment relation and can be denoted by $\mathcal{L} = \{\mathbb{P},\vDash\}$.

4.2.2 First-order Logic

4.2.2.1 Syntax

First-order logic[2] (FOL) is used to model the trust ecosystem introduced later in this thesis, which we denote by $\mathcal{TE}$.

FOL uses quantified variables and allows the use of sentences that contain variables. Thus, rather than propositions such as 'Aristotle is a man', one can have expressions in the form 'there exists X such that X is Aristotle and X is a man'. The expression *there exists* is a quantifier while X is a variable. This distinguishes first order logic from propositional logic, which does not use quantifiers or relations. Propositional logic can be seen as the foundation of first order logic.

FOL consists of sets of symbols for constants, variables, functions and predicates. Constants are used to refer to certain elements of the domain of interest, and are specified in uppercase. Variables are used as place holders, and are specified in lowercase. Functions are a particular form of relation (set of pairs), where each domain element has only one corresponding range element. Functions may be nested. The term predicate has various uses in logic. Here it is used to refer to relations, including properties.

The symbols $\exists$ and $\forall$ represent the traditional quantifiers *there exists* and *for all* in first-order logic. $\exists!$ expresses the uniqueness quantification. When sets are used, the symbols have their usual meaning, including the symbol | which is used to characterise the elements of a set.

Following Hitzler et al. [148], a *signature* (*V, C, F, P*) of a first-order language consists of sets of variables *V*, constant symbols *C*, function symbols *F* and predicate symbols *P*, where functions and predicates are associated with a non-negative integer known as its arity[3].

From this basis, terms and formulae can be defined inductively. Variables such as t are terms, and if f is a function symbol with arity k, then $f_{[t_1,\ldots,t_k]}$ is also a term.

[2]First-order logic is also known as predicate logic or quantificational logic.

[3]Arity is the number of arguments or operands that a function or predicate takes.

Formulae can also be defined inductively. If p is a predicate symbol with arity k, then $p_{[t_1,\ldots,t_k]}$ is an atomic formula. If F is a formula, then $\neg F$ is also. Conjunction and disjunction of formulae are defined using $\wedge$ and $\vee$. A formula does not need to be true.

The set of all first-order predicate logical formulae over (*V, C, F, P*) is called the first-order language over (*V, C, F, P*).

A sentence is defined as a first-order predicate logical formula in which all variable occurrences are bound. Bound means that substitution may no longer take place. A theory is a set of sentences. For a more detailed treatment see Barwise [24].

Predicate logic can be realised with or without equality. In a realisation with equality, there is a relationship symbol that represents the identity relation. The symbol = is typically used for this purpose. The symbol $\neq$ represents its opposite. For a more detailed treatment see Kresel and Krivine [206].

4.2.2.2 Translation into logic

To formalise reasoning that is described in natural language in logic requires a form of adaptation to which we refer here as translation. There is no fixed prescribed way for performing this translation. However the four statements described by Aristotle [9] and known as Aristotelian forms are well-known and form a common basis for such translation. They are:

- all *P*s are *Q*s, translated as $\forall x\ (P(x) \rightarrow Q(x))$,
- no *P*s are *Q*s, translated as $\forall x\ (P(x) \rightarrow \neg\ Q(x))$,
- some *P*s are *Q*s, translated as $\exists x\ (P(x) \wedge Q(x))$,
- some *P*s are not *Q*s, translated as $\exists x\ (P(x) \wedge \neg\ Q(x))$.

These forms can be combined, allowing the following examples of translations

- 'everyone loves someone else' as

  $\forall p\ (Person(p) \rightarrow \exists\ q\ (Person(q) \wedge p \neq q \wedge Loves(p,q)))$, and
- 'there is someone everyone else loves' as

  $\exists p\ (Person(p) \wedge \forall q(Person(q) \wedge p \neq q \rightarrow Loves(p,q)))$.

4.2.2.3 Semantics

Using FOL, the validity of an argument is determined by its logical form, not by its content. That is, validity is solely determined by the form, and not by the content of the arguments. However,

when studying meaning, it is common to use the representation $\mathcal{A} \vdash \mathcal{B}$ for the case where $\mathcal{B}$ can be syntactically derived from $\mathcal{A}$, and $\mathcal{A} \vDash \mathcal{B}$ for the case where $\mathcal{B}$ follows semantically from $\mathcal{A}$.

What is understood by the term *follows semantically* needs to be defined. For propositional logic this is simply an assignment of truth values to each of the atomic formulae present in the formula. However, for more complex logics, this is insufficient because, for example, quantifiers may need to be considered. Defining the semantics of FOL is a broad topic. As this thesis employs a Description Logic (DL), a particular type of FOL, for modelling, the semantics of DL are addressed in more detail in Section 4.3.3.

4.3 Semantic web formalisms

4.3.1 Resource Description Framework

4.3.1.1 Specification

The W3C defined RDF[4] as a standard model for data interchange on the Web. RDF is a framework for expressing information about resources, which can include documents, people, physical objects, and abstract concepts. The W3C published the first RDF specification, the 'Model and Syntax Specification' [333] in 1999. This describes the RDF data model and an XML serialisation. This was replaced in 2004 by a set of six specifications [337], [336], [340], [338], [339], [341] establishing RDF 1.0. These were superseded in 2014 by the following documents defining RDF 1.1, the current version.

- RDF 1.1 Primer [359] provides the knowledge required to use RDF. It introduces the basic concepts of RDF and provides concrete examples of the use of RDF.
- RDF 1.1 Concepts and Abstract Syntax [358] defines an abstract syntax (a data model) which serves to link all RDF-based languages and specifications. The abstract syntax has two key data structures. RDF graphs are sets of subject-predicate-object triples, where the elements may be Internationalised Resource Identifiers (IRIs), blank nodes, or datatyped literals; they are used to express descriptions of resources. RDF datasets are used to organise collections of RDF graphs, and comprise a default graph and zero or more named graphs. Key concepts and terminology are also introduced, and datatyping and the handling of fragment identifiers in IRIs within RDF graphs are discussed.
- RDF 1.1 XML Syntax [363] defines an XML syntax for RDF called RDF/XML; it consists of Namespaces in XML, the XML Information Set and XML Base.

[4] `https://www.w3.org/RDF/`

- RDF 1.1 Semantics [361] describes a precise semantics for RDF 1.1. It gives a number of distinct entailment regimes and corresponding patterns of entailment. It defines a model-theoretic semantics for RDF graphs and the RDF and RDFS vocabularies, providing an exact formal specification of when truth is preserved by transformations of RDF or operations which derive RDF content from other RDF.
- RDF Schema 1.1 [360] provides a data-modelling vocabulary for RDF data. RDF Schema is an extension of the basic RDF vocabulary.
- RDF 1.1 Test Cases [362] lists the test suites and implementation reports for RDF 1.1 Semantics as well as the various serialization formats.

4.3.1.2 RDF features

RDF is intended for use in situations in which information on the Web needs to be processed by applications, rather than only being displayed to people. RDF provides a framework for expressing this information so that it can be exchanged between applications without loss of meaning.

The RDF data model is based upon the idea of making statements about resources (in particular web resources) in the form of subject-predicate-object expressions. In RDF terminology these expressions are known as *triples*. The subject denotes the resource, and the predicate denotes traits or aspects of the resource and expresses a relationship between the subject and the object. For example, one way to represent the notion 'The sky has the color blue' in RDF is as the following triple: a subject denoting 'the sky', a predicate denoting 'has the color', and an object denoting 'blue'. A set of triples can be represented in the form of a directed graph, where the nodes represent subjects and objects, and a directed edge from subject to object represents a predicate. Such graphs can be merged. The W3C semantic web wiki[5] provides a starting point for further information.

It it interesting to observe that RDF swaps uses of the words object for subject as they are used in the terminology of an entity–attribute–value model within object-oriented design, where one would refer to object (sky), attribute (color) and value (blue).

4.3.1.3 Examples of use

RDF is used in a variety of settings.

- DBPedia[6] makes the content of Wikipedia[7] available in RDF.

[5] `https://www.w3.org/2001/sw/wiki/Main_Page`
[6] `https://wiki.dbpedia.org/`
[7] `https://www.wikipedia.org/`

- In the United Kingdom, The National Archives publish all UK legislation[8] on behalf of HM Government. The legislation is published in various formats including RDF[9].
- Also in the United Kingdom, 'The Gazette'[10] is an official journal of record which consists largely of statutory notices. It was established in 1665 and is published by The Stationery Office (TSO) under the superintendence of Her Majesty's Stationery Office (HMSO), part of The National Archives. Its data is published in various formats[11] including RDF.
- The regional government of Flanders publishes[12] its Central Address Reference Database, the decisions of local government entities and the register of Flemish public entities, in RDF.

For more applications of RDF and semantic web technology see Hitzler et al. [148], Chapter 9.

4.3.1.4 Syntax and semantics

RDF models can be expressed using a number of syntaxes [363] including N3, N-triples, Turtle (Terse RDF Triple Language) and RDF/XML.

RDF semantics can be defined intuitively in the following way.

- The Internationalised Resource Identifiers (IRIs) used to name the subject, predicate, and object are 'global' in scope, i.e. they name the same thing each time they are used.
- Each triple is 'true' exactly when the predicate relation exists between the subject and the object.
- An RDF graph is 'true' exactly when all the triples in it are 'true'.

The model-theoretic semantics for RDF graphs and the RDF and RDFS vocabularies [361] describe a precise semantics for RDF 1.1. RDF is intended for use as a base notation for notations such as OWL, whose expressions can be encoded as RDF graphs which use a particular vocabulary with a defined meaning. Also, particular IRI vocabularies may be given meanings by other specifications or conventions.

One of the benefits of RDF having declarative semantics is that logical inferences can be made. That is, given a certain set of input triples which are accepted as true, systems can in

[8] `http://www.legislation.gov.uk/`
[9] `http://www.legislation.gov.uk/developer/formats`
[10] `https://www.thegazette.co.uk/`
[11] `https://www.thegazette.co.uk/data/formats`
[12] `https://overheid.vlaanderen.be/oslo-datavlaanderen`

some circumstances deduce that other triples must, logically, also be true. It is said that the first set of triples entails the additional triples. The inference is calculated by a reasoner, which can also sometimes deduce that the given input triples contradict each other. Many different kinds of reasoning are possible, and a collection of types of reasoning forms what is known as an entailment regime. Several entailment regimes are specified in the RDF Semantics [361]. Additional SPARQL entailment regimes [364] specify which entailment relation is used, which queries and graphs are well-formed for the regime, how the entailment is used, and what kinds of errors can arise.

W3C also published the RDFS recommendation [360], specifying RDF Schema (RDFS), a vocabulary to express schema knowledge. It complements RDF's type definition `rdf:type` with an `rdfs:class` definition. This allows class hierarchies and more refined semantics. Hitzler et al. [148] provides a description of the model-theoretic semantics for RDFS.

4.3.2 SPARQL

4.3.2.1 SPARQL defined

SPARQL[13] is an RDF query language, i.e. it is a semantic query language to retrieve and manipulate data stored in RDF format. It was standardised by the RDF Data Access Working Group (DAWG) of the W3C. The current version is SPARQL 1.1 [367]. The specifications consist of the following documents.

- SPARQL 1.1 Query Language [369] — the description of the SPARQL query language for RDF;
- SPARQL Query Results XML Format [372], SPARQL 1.1 Query Results JSON Format [371] and SPARQL 1.1 Query Results CSV and TSV Formats [370] — apart from the standard SPARQL query results in XML Format, JavaScript Object Notation (JSON), Comma Separated Values (CSV) and Tab Separated Values (TSV) formats are allowed for query answers;
- SPARQL 1.1 Federated Query [365] — a specification defining an extension of the SPARQL 1.1 Query Language for executing queries distributed over different SPARQL endpoints;
- SPARQL 1.1 Entailment Regimes [364] — a specification defining the semantics of SPARQL queries under entailment regimes such as RDF Schema, OWL, or RIF;
- SPARQL 1.1 Update Language [375] — an update language for RDF graphs, allowing insertion and deletion of data from graphs, as well as graph management;

[13] a recursive acronym for SPARQL Protocol and RDF Query Language

- SPARQL 1.1 Protocol for RDF [368] — a protocol defining means for conveying arbitrary SPARQL queries and update requests to a SPARQL service;
- SPARQL 1.1 Service Description [373] — a specification defining a method for discovering and a vocabulary for describing SPARQL services;
- SPARQL 1.1 Graph Store HTTP Protocol [366] — as opposed to the full SPARQL protocol, this specification defines minimal means for managing RDF graph content directly via common HTTP operations;
- SPARQL 1.1 Test Cases [374] — a suite of tests for understanding corner cases in the specification and assessing whether a system is SPARQL 1.1 conformant.

4.3.2.2 Queries, the heart of SPARQL

SPARQL allows a query to consist of triple patterns, conjunctions, disjunctions, and optional patterns. Four query forms are supported:

- SELECT, which extracts values from a SPARQL endpoint, returning the results in a table format.
- ASK, which provides a True/False result for a query on a SPARQL endpoint.
- DESCRIBE, which extracts an RDF graph from the SPARQL endpoint, the content of which is left to the endpoint to decide based on what the maintainer deems as useful information.
- CONSTRUCT, which extracts information from the SPARQL endpoint and transforms the results into valid RDF.

4.3.3 Description Logics

4.3.3.1 Introduction

Description Logics are based on FOL. They were developed with the goals of providing formal, declarative meanings to semantic networks and frames, and of showing that such representation structures can be equipped with efficient reasoning tools. Baader et al. [16] provides a treatment of the formal aspects and evolution of DLs. DLs build on cognitive notions such as network structures and rule-based representations derived from experiments on recall from human memory and human execution of tasks such as puzzle solving. Information is modelled as network structures, where the structure of the network represents sets of individuals and their

relationships. The basic elements of a DL are unary predicates, denoting sets of individuals, and binary predicates, denoting relationships between individuals.

According to Baader et al. [16], the following evolution took place.

- Research in the area of DLs began under the label terminological systems, emphasising that the representation language was used to establish the basic terminology adopted in the modeled domain.
- Later the emphasis shifted to the set of concept-forming constructs admitted in the language, giving rise to the name concept languages.
- As attention moved further towards the properties of the underlying logical systems, the term Description Logics became popular. Over time the formal and computational properties of reasoning (such as decidability and complexity) of various description formalisms have been investigated in detail.
- Network-based representation structures were studied, formalising the elements of a network into nodes and links. Nodes are used to characterise concepts, i.e. sets or classes of individual objects, and links are used to characterise relationships amongst them.
- In some cases, more complex relationships are themselves represented as nodes; these are distinguished from nodes representing concepts. In addition, concepts can have simple properties, often called attributes, which are typically attached to the corresponding nodes.
- In much of the early work both individual objects and concepts were represented by nodes. Properties were usually called roles, expressed by a link from the concept to a node for the role. A precise characterisation of the meaning of a network can be given by defining a language for the elements of the structure and by providing an interpretation for the strings of that language.

4.3.3.2 Semantics

The basic concepts of semantics were introduced in 4.2.2.3. For propositional logic the definition of the term *follows semantically* is simply an assignment of truth values to each of the atomic formulae present in the formula.

For DLs, the definition of the term *follows semantically* is more complex because an assignment of truth values to each of the atomic formulae present in the formula is insufficient because variables and quantifiers ($\exists$, $\forall$) also need to be taken into account

For such logics, defining formal semantics involves providing a consequence relation that determines whether an axiom logically follows from a given set of axioms. This is achieved in

a model-theoretic way, making use of the concept of an interpretation. This can be summarised as follows.

- An interpretation consists of an interpretation domain and an interpretation function.
- The purpose of the interpretation function is to determine whether axioms are satisfied.
- This satisfaction is used to define the consequence relation.

Interpretation At syntactic level the signature of a DL defines its vocabulary, which contains the names of individuals, concepts and roles. Elements from the vocabulary can be used to formulate axioms. Interpretation is defined at a semantic level. An interpretation is normally denoted by $\mathcal{I}$ and consists of

- the domain $\triangle^I$ that contains all individuals existing in the world that $\mathcal{I}$ represents, and
- an interpretation function $.^I$ that maps the syntactical elements (the names of individuals, concepts and roles) to $\triangle^I$ by providing
  - for each individual name $a \in \mathrm{N}_\mathcal{I}$ a corresponding individual $\mathrm{a}^I \in \triangle^I$,
  - for each concept name $C \in \mathrm{N}_C$ a corresponding set $\mathrm{C}^I \subseteq \triangle^I$ (C^I is allowed to be empty),
  - for each role name $r \in \mathrm{N}_\mathcal{R}$ a corresponding set r^I of ordered pairs of domain elements.

This is illustrated in Figure 4.1.

As an example, consider the following signature:

- the set of individual names $\mathrm{N}_\mathcal{I}$ = {Europe, Africa, Asia, North_America, South_America, Atlantic, Indian, Pacific}
- the set of concept names N_C = {Continent, Ocean}
- the set of role names $\mathrm{N}_\mathcal{R}$ = {liesNorthOf, liesEastOf}

An interpretation $I = (\triangle^I, .^I)$ is defined as follows. Let the domain $\triangle^I$ contain the following elements: α, β, γ, δ, ϵ, ζ, א, ב, ג. Let the interpretation function $.^I$ be defined as:

- Europe.^{I} = α, Africa.^{I} = β, Asia.^{I} = γ, North_America.^{I} = δ, South_America.^{I} = ϵ
- Atlantic.^{I} = א, Indian.^{I} = ב, Pacific.^{I} = ג
- Continent.^{I} = {α, β γ, δ, ϵ }, Ocean.^{I} = {א, ב, ג }
- liesNorthOf.^{I} ={(α, β), (δ, ϵ)}, liesEastOf.^{I} ={(א, α), (א, β), (δ, ג) }

This is illustrated in Figure 4.2.

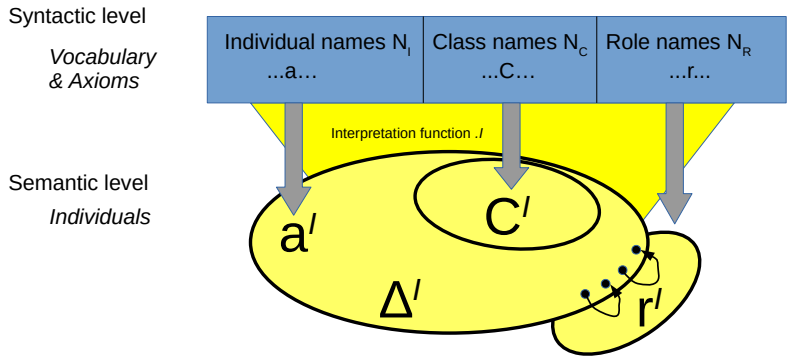

Figure 4.1: Structure of DL interpretation

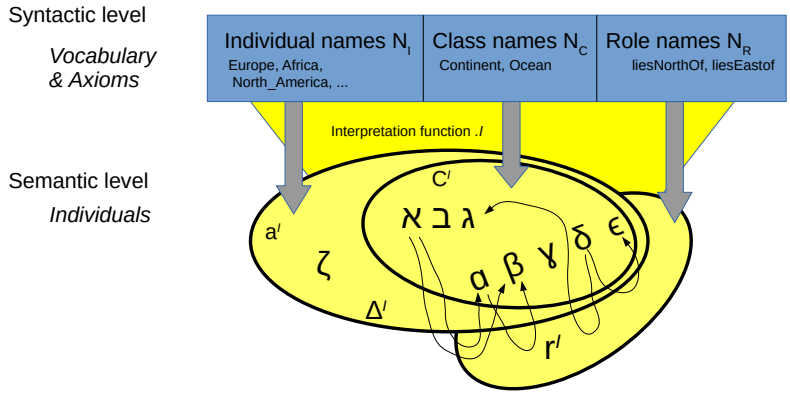

Figure 4.2: Illustration of the structure of a DL interpretation

Satisfaction of axioms To determine the semantics of a DL it is not only necessary to determine the truth of simple vocabulary elements such as individual names, but also of concepts, roles and axioms. Rudolph [282] defines how this can be done by extending the interpretation function $.^I$ to complex expressions. This approach can be summarised as follows.

- The interpretation function is extended from role names to roles by introducing the universal role which connects any two individuals of the domain, and also every individual with itself. The inverted role and its interpretation are also defined.

- The interpretation function for concepts is defined by describing
  - the additional concepts of $\top$ (the concept which is true for every individual) and $\bot$ (the concept which has no instances),
  - the interpretation of sets,
  - the interpretation of $\neg C$, $C \sqcap D$, $C \sqcup D$, quantifiers $\forall R.C$, $\exists R$, $\exists R$.self
  - the interpretation of $\leqslant nr.C$ and $\geqslant nr.C$

Whether an axiom holds given a specific interpretation is defined by describing how

- axioms for role inclusion and disjointness hold,
- the axiom for general concept inclusion holds,
- axioms for assertion of concepts and roles hold.

When an axiom α holds for a specific interpretation $\mathcal{I}$ it is said that $\mathcal{I}$ is a model of α or that $\mathcal{I}$ satisfies α, written $\mathcal{I} \vDash \alpha$. Once an interpretation $\mathcal{I}$ is defined as a model of an axiom, this notion can be extended to entire knowledge bases. $\mathcal{I}$ is a model of a given knowledge base $\mathcal{KB}$ (or $\mathcal{I}$ satisfies $\mathcal{KB}$, written $\mathcal{I} \vDash \mathcal{KB}$) if it satisfies all the axioms of $\mathcal{KB}$, i.e. if $\mathcal{I} \vDash \alpha$ for every $\alpha \in \mathcal{KB}$. A knowledge base is called satisfiable or consistent if it has a model, and unsatisfiable or inconsistent otherwise.

Consequence relation The consequence relation determines whether an axiom is true with respect to an interpretation. It is commonly denoted by $\vDash$ and is defined as follows. An axiom α is a consequence of (or *entailed by*) a knowledge base $\mathcal{KB}$ (written $\mathcal{KB} \vDash \alpha$) if every model of $\mathcal{KB}$ is also a model of α. That is, if for every $\mathcal{I}$ with $\mathcal{I} \vDash \mathcal{KB}$ it also holds that $\mathcal{I} \vDash \alpha$.

For a detailed treatment see Rudolph [282] or Hitzler et al. [148]. Rudolph discusses the details of DL knowledge bases including their syntax, semantics and reasoning capabilities. Hitlzer presents model-theoretic semantics of the OWL DL, and a translation of it into FOL predicates.

4.3.3.3 Open World Assumption

The non-finiteness of the domain and the open-world assumption (OWA) are distinguishing features of DLs with respect to the modelling languages developed in the study of databases.

Hitzler et al. [148] defines OWA as the complement of the closed world assumption (CWA). The CWA states that everything which is not explicitly true is deemed to be false. Conventional databases are interpreted under the CWA. That is, if something is not stated in the database, it

is assumed not to be the case. The OWA leaves such things undefined; if it not stated whether or not something is the case, then under the OWA it is assumed to be unknown. The OWA is not formally defined, but RDF(S) and DLs such as OWL adhere to it.

Monotonicity of entailment is a property of logical systems that means that the hypotheses of any derived fact may be freely extended with additional assumptions. Monotonic logics adhere to the OWA.

4.3.3.4 Inference

The basic means of inference on concept expressions in DLs is subsumption, typically written as C $\sqsubseteq$ D. Determining subsumption is the problem of checking whether the concept denoted by C (the subsumee) is less general than the one denoted by D (the subsumer). In other words, subsumption checks whether the first concept always denotes a subset of the set denoted by the second.

4.3.4 Knowledge representation and the Attributive Language $\mathcal{AL}$

4.3.4.1 Tbox and Abox

A DL knowledge base typically contains components of two types, referred to as TBox and ABox. The TBox contains intensional knowledge in the form of a terminology (hence the term TBox) and is built through declarations that describe general properties of concepts. Because of the nature of the subsumption relationships among the concepts that constitute the terminology, TBoxes are usually thought of as having a lattice-like structure; this mathematical structure arises from the subsumption relationship, and has nothing to do with any implementation. The ABox contains extensional knowledge, also called assertional knowledge (hence the term ABox), i.e. knowledge that is specific to the individuals of the domain of discourse.

4.3.4.2 DL languages

DLs are subsets of first-order logic, as discussed by Borgida [36]. For practical purposes, decidable fragments of FOL are most relevant. The languages used to express DLs are distinguished by the constructors they provide. The foundational language is $\mathcal{AL}$ (Attributive Language), introduced in 1991 [289] as a minimal practical language. The other languages of this family are extensions of $\mathcal{AL}$. Concept descriptions in $\mathcal{AL}$ are formed according to the following syntax rule:

$C, D \longrightarrow A \mid \neg A \mid \top \mid \bot \mid C \sqcap D \mid \forall R.C \mid \exists R.\top$

A family of $\mathcal{AL}$ languages can be defined by adding additional constructors. The union of concepts is written as $\sqcup$ and is indicated by the letter $\mathcal{U}$. Full existential qualification is written

as $\exists R.C$ and is indicated by the letter $\mathcal{E}$. This is different from limited existential qualification in that arbitrary concepts are now allowed to occur in the scope of the existential quantifier (rather than only $\top$).

Number restrictions are indicated by the letter $\mathcal{N}$ and are written as $\geq nR$ (at-least restriction) and $\leq nR$ (at-most restriction), where n ranges over the non-negative integers. The negation of arbitrary concepts (indicated by the letter $\mathcal{C}$ for complement) is written as $\neg C$.

Extending $\mathcal{AL}$ by any subset of these constructors yields a particular $\mathcal{AL}$-language. These are named using a string of the form $\mathcal{AL}[\mathcal{U}][\mathcal{E}][\mathcal{N}][\mathcal{C}]$, where a letter in the name stands for the presence of the corresponding constructor. From the semantic point of view, however, these languages are not all distinct. The semantics enforce the equivalences $C \sqcup D \equiv \neg(\neg C \sqcap \neg D)$ and $\exists R.C \equiv \neg\forall R.\neg C$. Hence, union and full existential quantification can be expressed using negation. It is customary to write the letter $\mathcal{C}$ instead of the letters $\mathcal{UE}$ in language names. So $\mathcal{ALC}$ is written instead of $\mathcal{ALUE}$, and $\mathcal{ALCN}$ instead of $\mathcal{ALUEN}$.

4.3.4.3 The DL $\mathcal{SROIQ}$

Many different description logics have been introduced, characterised by the types of constructors and axioms that they allow. These are often a subset of the constructors in the language known as $\mathcal{SROIQ}$. For a description of $\mathcal{SROIQ}$, including its decidability, see Horrocks et al. [153].

The description logic $\mathcal{ALC}$ is the fragment of $\mathcal{SROIQ}$ that allows no RBox axioms and only $\sqcap$, $\sqcup$, $\neg$, $\forall$ and $\exists$ as its concept constructors. It is often regarded as the most basic DL; see for example Hitzler et al. [148].

The extension of $\mathcal{ALC}$ with transitive roles is traditionally denoted by the letter $\mathcal{S}$. Some other letters used in DL names hint at a particular constructor, such as inverse roles $\mathcal{I}$, nominals $\mathcal{O}$, qualified number restrictions $\mathcal{Q}$, and role hierarchies (role inclusion axioms without composition) $\mathcal{H}$. For example, the DL named $\mathcal{ALCHIQ}$ extends $\mathcal{ALC}$ with role hierarchies, inverse roles and qualified number restrictions. The letter $\mathcal{R}$ commonly refers to the presence of role inclusions ($\sqsubset$ indicates inclusion), local reflexivity Self, and the universal role U, as well as the additional role characteristics of transitivity, symmetry, asymmetry, role disjointness, reflexivity, and irreflexivity. This naming scheme explains the name $\mathcal{SROIQ}$, the DL central to this thesis and which is discussed next.

4.3.5 The Description Logic $\mathcal{SROIQ}(\mathcal{D})$

4.3.5.1 Defining $\mathcal{SROIQ}(\mathcal{D})$

In this thesis, the Description Logic $\mathcal{SROIQ}(\mathcal{D})$ is used to describe the concepts required to formulate trust claim interpretations. $\mathcal{SROIQ}(\mathcal{D})$ adds the following to $\mathcal{ALC}$, observing that

the term role is frequently used as a synonym for property.

- Role chains express, as their name implies, a chaining of roles. A simple example of chaining is provided by *hasParent* $\circ$ *hasBrother* $\sqsubseteq$ *hasUncle*. In predicate logic this can be expressed as $\forall x\ \forall y$ *(*$\exists z$ *((hasParent(x,z)* $\wedge$ *hasBrother(z,y))* $\rightarrow$ *hasUncle(x,y)))*. This is denoted by $\mathcal{ALC}$ + role chains = $\mathcal{SR}$.
- Transitivity, for which *hasAncestor* $\circ$ *hasAncestor* $\sqsubseteq$ *hasAncestor* provides a straightforward example.
- Role hierarchies, for which *hasFather* $\sqsubseteq$ *hasParent* provides a simple example. This is denoted by $\mathcal{SH}$ = $\mathcal{S}$ + role hierarchies.
- Nominals are used to create closed classes. A simple example of such creation of closed classes is provided by *MyBirthdayGuests* $\equiv$ *{Danny, Brendan, Steven, Els}*. This is denoted by $\mathcal{O}$.
- Individual equality and inequality, without the unique name assumption. An example thereof is provided by *Danny = Godot* hence *{Danny}* $\equiv$ *{Godot}*, and *Danny* $\neq$ *Godot* hence *{Danny}* $\sqcap$ *{Godot}* $\equiv \bot$.
- Inverse roles, for which *hasParent equiv* $hasChild^-$, and *Orphan* $\equiv hasChild^-.Dead$ provide an example.
- Qualified cardinality restrictions, such as *Car* $\sqsubseteq$ *= 4hasTyre.*$\top$.
- Roles can be declared to be transitive, symmetric, asymmetric, reflexive, irreflexive, functional (can only take one value) and inverse functional. This is referred to as role characteristics.
- Datatypes, which allows datatype literals. This is denoted by $\mathcal{D}$.
- Capabilities to express
  - Self, illustrated by *PersonCommittingSuicide* $\equiv \exists$*kills.Self*.
  - Disjointness of properties, illustrated by *Disjoint(hasParent, hasChild)*.
  - Anonymous individuals, instead of named individuals.

4.3.5.2 $\mathcal{SROIQ}(\mathcal{D})$ constructors

$\mathcal{SROIQ}$ offers constructors as basic building blocks, which can be assembled into axioms. Syntax and semantics are defined for constructors (concepts, roles and individuals) as well as

for axioms (T-, R- and A-boxes). Constructors exist for individuals, roles and concepts. Axioms are combined to form a Knowledge Base, alternatively referred to as an ontology.

Every ontology is based on three finite sets of signature symbols: the set N_C of concept names, the set N_R of role names, and the set N_I of individual names. The set of $\mathcal{SROIQ}$ role expressions R over this signature is defined by $R ::= U|N_R|N_{R^-}$ where U is the universal role which always relates all pairs of individuals. Concepts can be created using disjunction, conjunction, negation, universal restriction and existential restriction. Two specific class names, $\top$ (top) and $\bot$ (bottom), denote the concept containing all individuals and the empty concept, respectively.

Formally, the set of $\mathcal{SROIQ}$ concept expressions is defined as $C ::= N_C \mid (C \sqcap C) \mid (C \sqcup C) \mid \neg C \mid \top \mid \bot \mid \exists R.C \mid \forall R.C \mid \geq nR.C \mid \leq nR.C \mid \exists R.Self \mid \{N_I\}$ where n is a non-negative integer.

4.3.5.3 Using $\mathcal{SROIQ}(D)$ to build a Knowledge Base

A $\mathcal{SROIQ}$ Knowledge Base (KB) is a set of axioms consisting of terminological (T- and R-boxes) and assertional (A-boxes) parts. The T-boxes capture the terminology and universal statements of the modelled domain. R-boxes capture roles. A-boxes include concept assertions (such as *Musician(David)*), datatype property assertions (such as *:hasAge :David "21"^^xsd:integer)* and role assertions (such as *Married(David, Iman)*). The semantics of a KB take into account all possible situations in which the axioms would hold. This is referred to as the *Open World Assumption*. Unspecified information is kept open rather than being allocated a default value. The more axioms an ontology with a finite domain contains, the more constraints it imposes on its interpretations, and the fewer interpretations exist that satisfy all axioms. An interpretation $\mathcal{I}$ consists of a set called the interpretation domain $\triangle^I$, and an interpretation function $.^I$. The interpretation function $.^I$ maps a concept name A to a subset A^I of $\triangle^I$, a role name R to a binary relation R^I over $\triangle^I$, and an individual name i to an element i^I of $\triangle^I$.

For a KB to be free of inconsistencies and modelling errors, there should be at least one interpretation that satisfies all the axioms. Such a KB is called consistent, and such an interpretation is called a model of the ontology. To ensure the existence of reasoning algorithms that are correct and terminating, additional restrictions must be placed on the syntax. These are called structural restrictions, since they apply to the entire set of axioms. For $\mathcal{SROIQ}$ these restrictions are simplicity and regularity. Simplicity enforces some restrictions on disjointness of roles and on concept expressions. Regularity enforces some restrictions on R-boxes to limit cyclic dependencies between them.

Once a KB $\mathcal{K}$ is created, inference is possible to verify whether $\mathcal{K}$ captures the intended entailments, expressed as $C \subseteq D$ with regard to $\mathcal{K}$ iff for every model $\mathcal{I}$ of $\mathcal{K}$, $C^I \subseteq D^I$. Furthermore it is possible to verify that:

- $\mathcal{K}$ is consistent, i.e. it is possible to have at least one interpretation that satisfies all axioms;
- $\mathcal{K}$ is minimally redundant, i.e. there are no unintended synonyms, expressed as C is equivalent to D with regard to $\mathcal{K}$ iff for every model $\mathcal{I}$ of $\mathcal{K}$, $C^I = D^I$;
- $\mathcal{K}$ is meaningful, i.e. concepts can have individuals, expressed as C is satisfiable with regard to $\mathcal{K}$ iff there exists some model $\mathcal{I}$ of $\mathcal{K}$ such that $C^I \neq \emptyset$.

$\mathcal{K}$ can then be queried to learn:

- the subsumption hierarchy of all atomic concepts;
- all the individuals known to be instances of a certain concept;
- whether $\mathcal{K}$ entails a certain axiom $C(a)$;
- whether a given concept is (un)satisfiable;
- whether x is an instance of C with regard to $\mathcal{K}$ iff for every model $\mathcal{I}$ of $\mathcal{K}$, $x^I \in C^I$;
- (x,y) is an instance of R with regard to $\mathcal{K}$ iff for every model $\mathcal{I}$ of $\mathcal{K}$, $(x^I, y^I) \in R^I$.

For a more detailed treatment see Hitzler et al. [148].

4.3.5.4 OWA revisited

An analogy can be established between databases and DL knowledge bases. The schema of a database can be compared to the TBox, and the instance incorporating the actual data to the ABox. However, the semantics of ABoxes differs from the usual semantics of database instances. While a database instance represents exactly one interpretation, namely the one in which classes and relations in the schema are interpreted by the objects and tuples in the instance, an ABox represents many different interpretations, namely all its models. As a consequence, absence of information in a database instance is interpreted as negative information, while absence of information in an ABox only indicates lack of knowledge. That is, while the information in a database is always deemed to be complete, the information in an ABox is in general viewed as being incomplete. The semantics of ABoxes is therefore sometimes characterised as 'open-world' semantics, while the traditional semantics of databases is characterised as 'closed-world' semantics. For a detailed discussion of this issue see Baader [16].

4.3.6 The W3C Web Ontology Language (OWL)

4.3.6.1 OWL 1

The possibility of viewing the World-Wide Web as a semantic network has been considered since the advent of the Web itself. The concept of an ontology was generally accepted as useful for this purpose, and is loosely defined as a model which represents some subject matter.

W3C standardised a Web Ontology Language based on the $\mathcal{SROIQ}(\mathcal{D})$ description logic and called it OWL. This became a W3C recommendation in February 2004 [335]. This version is also referred to as OWL 1.

It adds the notion of keys on top of $\mathcal{SROIQ}(\mathcal{D})$, which are a set of (object or data) properties whose values uniquely identify an object. OWL uses the open world assumption (if a fact is missing it may still be true, but simply missing), as opposed to the closed world assumption (if fact is not present in the data it is assumed to be false). An OWL ontology maps to a DL knowledge base, Tbox, RBox and Abox.

OWL is a family of three language variants (often called species) of decreasing expressive power: OWL Full, OWL DL, and OWL Lite:

- OWL Full is the union of OWL syntax and RDF,
- OWL DL is restricted to a decidable FOL fragment,
- OWL Lite is an easier to implement subset of OWL DL.

Practical experience with OWL 1 has shown that OWL 1 DL lacks several constructs that are often necessary for modelling complex domains. OWL 1's lack of a suitable set of built-in datatypes is a particular shortcoming. OWL 1 relies on XML Schema (xsd) for the list of built-in datatypes.

4.3.6.2 OWL 2 Full and DL

The above issues were addressed in OWL 2, which improves the datatypes of OWL 1. Like OWL 1, OWL 2 is a declarative language, i.e. it describes a state of affairs in a logical way. For this it uses classes, properties, and individuals. Reasoners can then be used to infer further information about that state of affairs. How these inferences are realised is not part of the OWL specification, and the realisation depends on the specific implementation. Still, the correct answer to any such question is predetermined by the formal semantics, which comes in two versions: the Direct Semantics and the RDF-Based Semantics. Only implementations that comply with these semantics can be regarded as OWL 2 conformant.

OWL 2 [342] was published by the W3C in 2012 as a series of documents. It is normatively defined by five core specification documents:

- Structural Specification and Functional-Style Syntax [352] defines the constructs of OWL 2 ontologies in terms of both their structure and a functional-style syntax, and defines OWL 2 DL ontologies in terms of global restrictions on OWL 2 ontologies.
- Mapping to RDF Graphs [348] defines a mapping of the OWL 2 constructs into RDF graphs, and thus defines the primary means of exchanging OWL 2 ontologies in the Semantic Web.
- Direct Semantics [346] defines the meaning of OWL 2 ontologies in terms of a model-theoretic semantics.
- RDF-Based Semantics [351] defines the meaning of OWL 2 ontologies via an extension of the RDF Semantics.
- Conformance [343] provides requirements for OWL 2 tools and a set of test cases to help determine conformance.

Four additional specifications complement the core specifications:

- Profiles [350] defines three sub-languages of OWL 2 that offer advantages in particular applications scenarios.
- XML Serialisation [353] defines an XML syntax for exchanging OWL 2 ontologies, suitable for use with XML tools like schema-based editors and XQuery/XPath.
- Manchester syntax [347] defines an easy-to-read, but less formal, syntax for OWL 2 that is used in some OWL 2 user interface tools
- Data Range Extension: Linear Equations [344] specifies an optional extension to OWL 2 which supports advanced constraints on the values of properties.

Besides the Functional-Style syntax, the Manchester syntax and the XML Serialisation, in practice the Turtle syntax [345] is also used.

The OWL 2 Primer [349] defines two types of OWL 2, OWL 2 DL and OWL 2 Full, with corresponding semantics.

- The Direct Semantics provide meaning for OWL 2 DL in a Description Logic style. Informally, the term OWL 2 DL is often used to refer to OWL 2 ontologies interpreted using the Direct Semantics (but it is also possible to interpret OWL 2 DL ontologies under RDF-Based Semantics). As demonstrated by Hitzler et al. [148], OWL 2 DL corresponds to $\mathcal{SROIQ}$. Horrocks et al. [153] have shown that $\mathcal{SROIQ}$ is decidable. There are several production quality reasoners for OWL 2 DL[14].

[14] `http://owl.cs.manchester.ac.uk/tools/list-of-reasoners/`

- The RDF-Based Semantics provide meaning for OWL 2 Full. These semantics are an extension of the semantics for RDFS and is based on viewing OWL 2 ontologies as RDF graphs. OWL 2 Full is undecidable. There are no production quality reasoners for OWL 2 Full.

4.3.6.3 OWL 2 profiles

In addition to OWL Full and OWL DL, OWL 2 specifies three OWL sublanguages, referred to as profiles [350]. An OWL 2 profile (also called a fragment) is a trimmed down version of OWL 2 that trades some expressive power for efficiency of reasoning. Each profile achieves efficiency in a different way and is useful in different application scenarios. OWL 2 profiles are defined by placing restrictions on the structure of OWL 2 ontologies. The profiles are as follows.

- OWL 2 EL is useful in applications employing ontologies that contain very large numbers of properties and/or classes. This profile captures the expressive power used by many such ontologies and is a subset of OWL 2 for which the basic reasoning problems can be performed in time that is polynomial with respect to the size of the ontology. The EL acronym reflects the profile's basis in the EL family of description logics, referred to as EL++ [28], logics that provide only existential quantification.

- OWL 2 QL is aimed at applications that use very large volumes of instance data, and where query answering is the most important reasoning task. In OWL 2 QL, conjunctive query answering can be implemented using a conventional relational database system. As in OWL 2 EL, polynomial time algorithms can be used to implement the ontology consistency and class expression subsumption reasoning problems. The expressive power of the profile is necessarily quite limited, although it does include most of the main features of conceptual models such as UML class diagrams and ER diagrams. The QL acronym reflects the fact that query answering in this profile can be implemented by rewriting queries into a standard relational Query Language.

- OWL 2 RL is aimed at applications that require scalable reasoning without sacrificing too much expressive power. It is designed to accommodate OWL 2 applications that can trade the full expressivity of the language for efficiency, as well as RDF(S) applications that need some added expressivity. OWL 2 RL reasoning systems can be implemented using rule-based reasoning engines. The ontology consistency, class expression satisfiability, class expression subsumption, instance checking, and conjunctive query answering problems can be solved in time that is polynomial with respect to the size of the ontology.

The RL acronym reflects the fact that reasoning in this profile can be implemented using a standard Rule Language.

Another entailment regime was specified by ter Horst [309]. It is commonly referred to as OWL Horst. It addresses the possibilities from combining the standard Semantic Web languages RDF and OWL with facilities for expressing and reasoning with rules. OWL Horst extends the model theory of RDF with rules, while integrating OWL with a focus on the decidability of entailment and on its computational complexity.

4.3.6.4 OWL DLP

Grosof et al. [137] introduce Description Logic Programs (DLP) which combine rules with ontologies. DLP is defined by the intersection of RuleML Logic Programs and ontologies (in OWL/DAML+OIL Description Logic), and Description Horn Logic (DHL).

4.3.6.5 OWL DL as an implementation of $\mathcal{SROIQ}$

OWL DL is the syntactic fragment of OWL that abides by the restriction that OWL axioms can be read as $\mathcal{SROIQ}$ axioms for which the structural restrictions are satisfied. This means that once $\mathcal{SROIQ}$ constructors and axioms are identified, these are described in DL classes (unary predicates, corresponding to $\mathcal{SROIQ}$ concepts), and DL properties (binary predicates, corresponding to $\mathcal{SROIQ}$ roles). For a detailed treatment of the translation of a $\mathcal{SROIQ}$ KB into OWL DL classes and properties, see Rudolph [282].

OWL is a practical way to create and populate an ontology. It can be used to specify what kinds of things there are for the subject matter of interest, and how these are related to one another. The kinds of things are called classes. The concept of class in OWL is well defined and different from the concept of a class in object oriented programming. From a semantic perspective, an OWL class corresponds to a set. OWL allows class hierarchy, disjointness, and class equivalence to be defined. The term individual refers to an entity that is a member of a specific set.

The following class definitions are commonly used as an example. *Person* is a class which has two subclasses, *Patient* and *Doctor*. An individual can be a member of either of these classes. The set membership can be asserted (i.e. provided as a fact), or can be inferred on the basis of information that is already available. For example the class definition of *Patient* may impose no restrictions on class membership, i.e. it can be freely asserted that any entity which is a *Person* can be a *Patient*. However, the class of *Doctor* may define a *Doctor* as a *Person* with the imposed restriction that a *Doctor* must have the property of holding a medical degree.

Relations between resources are expressed by properties in OWL. From a mathematical perspective, a property is a set of ordered pairs. Semantics of a property can be defined us-

ing property hierarchies, domains and ranges, property characteristics (such as functional and transitive) and property inverses.

There are three types of properties: object properties, data properties and annotation properties. Object and data properties participate in inference, while annotation properties do not. An object property relates an individual to another individual. A data property relates an individual to a literal, so its range must be a datatype. Given a property has a value, the choice of using an object or a data property depends on whether there is a need to say something about that value. If there is such a need, the best choice is to use an object property, which allows the value to be the subject of a triple. If no such need exists, it is common to use a data property.

To continue the example above, a degree could be a class, of which a specific medical degree is an individual. The restriction that a Doctor must have a medical degree can then be expressed via an object property restriction. However, under the OWA, this does not mean that it is impossible to have an individual of the class Doctor that does not have a medical degree. This would become visible by querying the knowledge base appropriately.

4.3.6.6 Controlled vocabularies

The concept of 'controlled vocabulary' was introduced to normalise the diversity of semantics that can be expressed using RDF. However this does not allow the modelling of relationships beyond *broader*, *narrower* and *seeAlso* relations. For this purpose, RDF Schema and OWL provide mechanisms to formally represent a set of concepts and their relations, such as *is-a* relationship, or specific relations through so-called object properties.

In particular, OWL supports the creation of semantics through class and property hierarchies. Properties can have domains which say what class the subject of a triple using the property must be a member of, and ranges which say the same for the object of a triple. Properties can have characteristics such as being functional or transitive. Class expressions can be constructed using property restrictions and set operations. Property restrictions express what properties individuals of a given class have. Class equivalence and inference can be used to determine what classes an individual belongs to. An implementation of OWL includes an inference engine, which can detect logical inconsistencies within an ontology.

4.4 Summary

We introduced the background necessary to understand the capabilities and limitations of the model of claims and evaluations of trustworthiness which is introduced in the next chapter. This model is specified in OWL, a DL, which is a type of first-order logic. We first introduced notation for sets and logic, followed by that for first-order logic. The essential characteristics of first-order logic were discussed. Compared to the simpler propositional logic, first-order logic

adds ∃ and ∀ as quantifiers. This allows a broader set of situations to be captured. However it comes at the expense of a more complex syntax and semantics. It was also explained that what is understood by the term *follows semantically* needs to be defined. For propositional logic it is simply an assignment of truth values to each of the atomic formulae present in the formula. However, for first-order logic, this is insufficient because quantifiers need to be considered.

The specification and the implementation of the model described later in this thesis, have been performed using semantic web software which relies on RDF. This is a framework for creating a data model about resources, which can include documents, people, physical objects, and abstract concepts. It is based upon the idea of making statements about resources (in particular web resources) in the form of subject-predicate-object expressions, known as *triples*. The subject denotes the resource, and the predicate denotes traits or aspects of the resource and expresses a relationship between the subject and the object. A set of triples can be represented in the form of a directed graph, where the nodes represent subjects and objects, and a directed edge from subject to object represents a predicate. Such graphs can be merged. SPARQL is a semantic query language that can be used to retrieve and manipulate data stored in Resource Description Framework format. SPARQL allows a query to consist of triple patterns, conjunctions, disjunctions, and optional patterns.

The work described in this thesis employs OWL, which is based on the $\mathcal{SROIQ}$ DL, for modelling, and SPARQL for querying. The capabilities of DLs in general and of $\mathcal{SROIQ}$ in particular are a consequence of the types of constructors and axioms allowed. The characteristics of the $\mathcal{SROIQ}$ DL were described, as this is the basis for OWL which was used in our implementation. OWL allows the specification of what kind of things ('classes') there are for the subject matter of interest, and how these are related to one another. OWL allows the definition of class hierarchy, disjointness, and class equivalence. An individual is an entity that is a member of a class.

Relations between resources are expressed by properties in OWL. There are three types of properties: object properties, data properties and annotation properties. Object and data properties participate in inference, while annotation properties do not. An object property relates an individual to another individual. A data property relates an individual to a literal. The semantics of a property can be defined by using property hierarchies, domains and ranges, property characteristics (such as functional and transitive) and property inverses.

Part II

Modelling trustworthiness

Chapter 5

Requirements for trustworthiness

The goal of the work described in this thesis is to enable automated reasoning about the trustworthiness of entities; this requires an understanding of what must hold for an entity to be deemed trustworthy, the topic which forms the main focus of this chapter. We develop an integrated set of requirements for trust, i.e. things which must hold for an entity, or the outcome of an interaction, to be regarded as trustworthy. These trust requirements arise from two sources: the analysis in the structured literature review in Chapter 3, and the findings of the FutureTrust research project. We also compare these requirements with key elements of the research questions given in Section 1.2.3.

5.1 Introduction

As observed in Part I, trust is a term commonly used in natural language, is rooted in the social sciences and is open to many interpretations. There is no consensus to its meaning, either in the social sciences or elsewhere. The same holds for the term trustworthiness. We thus need to develop a definition of trustworthiness that is suitable for our purposes.

Identity is a fundamental pillar of trustworthiness. Given the size and complexity of this topic, it is outside the scope of the thesis except for those elements that are fundamental to the proposed framework. For this purpose, identity is addressed in Sections 5.4.2.1 and 7.5.3.

As described in Section 1.2.2, this thesis assumes that it is to the benefit of honest parties that the evaluation of a transaction is based on a model with semantics, reasoning and evidence understandable to all parties. Thus we take the approach of developing means to enable decisions on the basis of evidence and reasoning, based on an evaluation of trustworthiness. As a consequence, we focus on requirements for trustworthiness rather than for trust.

The requirements for assessing trustworthiness are based on the findings from the survey

described in Chapter 3 as well as on an elaboration of the requirements developed by the author in the FutureTrust project[1].

This chapter consists of the following sections. Section 5.2 introduces the objectives 'of this chapter, together with key assumptions and definitions. Section 5.3 describes the requirements that were formulated on the basis of the literature survey, and Section 5.4 describes the requirements derived from the FutureTrust project. Section 5.5 specifies an integrated set of requirements, based on the requirements given in the previous two sections. Section 5.6 summarises the chapter.

5.2 Definitions

5.2.1 Objective and assumptions

The objective of this chapter is to define requirements for a system to be defined and prototyped that supports the hypothesis given in Section 1.2.2, namely:

> *Where machine processable information about actors is available, it is desirable and possible to automate reasoning about the properties of these actors to support trust-related decision making based on formal semantics.*

In Section 1.2.3 a set of research questions was derived from these hypotheses, and the system described in later chapters of this thesis should help in answering these questions.

To allow the definition of requirements, we make the following two assumptions, necessary to allow the application of logical reasoning to trustworthiness.

- The trustworthiness of participants and interactions in an well-defined ecosystem can be deduced in a logical and transparent way from a set of unambiguously defined data points.
- Such an ecosystem and data points can be defined and implemented.

5.2.2 Defining trustworthiness

The following working definition of trustworthiness is used in the remainder of the thesis. Trustworthiness is a characteristic of an entity, where entities include persons, ICT systems, organisations and information artefacts, with the properties given below. An entity can be qualified as being ex-ante or ex-post trustworthy, as follows.

[1] FutureTrust is a European Commission Horizon 2020 project (grant 700542-Future-Trust-H2020-DS-2015-1), ref http://www.futuretrust.eu

- When an entity is qualified as ex-ante trustworthy this means a trustor can have reasonable expectations that future interactions and their outcomes will be consistent with what has been communicated or committed by the trustee. This is also called forward-looking trustworthiness.
- When an entity is qualified as ex-post trustworthy this means a trustor can have reasonable expectations that the outcome of a transaction performed in the past can be relied upon. This is also called backward-looking trustworthiness.

5.3 Requirements from the literature survey

The survey of Chapter 3 identified four questions as relevant for further research. As these questions indicate unmet needs, they were analysed to identify applicable elements for the creation of the requirements for the $\mathcal{TE}$ model introduced in the next chapter. The four questions are the following.

- How can we semantically define trustworthiness?
- How can we reason about trustworthiness?
- On what can reasoning to qualify an entity as trustworthy be based?
- How can we obtain information for use in supporting such reasoning about 'real world' entities?

The description of each question is given in Section 3.5.3. We now describe how inputs to the $\mathcal{TE}$ model requirements were derived from the questions identified by the survey.

5.3.1 SR1 Semantic definition of trustworthiness

The need to develop a broadly applicable semantic definition of trustworthiness was discussed in Section 3.5.3.1. This leads to Requirement SR1.

As a possible participant in an electronic interaction I can understand the meaning of trustworthiness of participants I plan to engage with, so that I can make an informed decision on whom to interact with.

5.3.2 SR2 Reasoning about trustworthiness

The need for an unambiguous method for reasoning about trustworthiness was discussed in Section 3.5.3.2. This leads to Requirement SR2.

As a possible participant in an electronic interaction I can understand the reasoning performed by a system that offers an evaluation of trustworthiness, so that I can verify this reasoning is compatible with the way I want to rely on its outcome.

5.3.3 SR3 Deciding whether an entity is trustworthy

The need to providing a means to decide whether an entity is trustworthy in a particular context was discussed in Section 3.5.3.3. This leads to Requirement SR3.

As a possible participant in an electronic interaction I can understand the arguments used in the reasoning that justify a participant is qualified as trustworthy, so that I can verify these arguments are compatible with the way I want to rely on the reasoning's outcome.

5.3.4 SR4 Information for reasoning about trustworthiness

The need for sources of information and appropriate types of information to input to a trustworthiness reasoning process was discussed in Section 3.5.3.4. This leads to Requirement SR4.

As a possible participant in an electronic interaction I can understand the information used in the reasoning that justify a participant is qualified as trustworthy, so that I can verify this information is compatible with the way I want to rely on the reasoning's outcome.

5.4 Requirements from FutureTrust

5.4.1 The FutureTrust project

5.4.1.1 Relationship between the thesis and the project

On the basis of the article *A Comparison of Trust Models* [295], I was invited to join the FutureTrust project, to work on a trust model. I participated in the project as lead author of two deliverables[2]

- Deliverable 2.5 On Trust and Trust Models [229];
- Deliverable 2.6 Evaluation Scheme for Trustworthy Services [230].

5.4.1.2 Project objectives

The requirements for trust and trustworthiness modelling developed in the FutureTrust[3] project were analysed, and applicable elements were selected.

[2]Both deliverables are available at the project website `https://www.futuretrust.eu/deliverables`.
[3]`https://www.futuretrust.eu/`

The FutureTrust project addressed the implementation of the eIDAS regulation [103]. The project received funding from European Union's Horizon 2020 research and innovation program under grant 700542. It was performed by eighteen participants and coordinated by Prof. J. Schwenk from the Ruhr-Universität Bochum. The project kick-off meeting was held in June 2016, and the project concluded in December 2020.

The core objective of the FutureTrust project was to support the implementation of the eIDAS regulation [103] on electronic identification (eID) and trusted services for electronic transactions in the internal market, and facilitate the widespread use of trustworthy eID and electronic signature technology in Europe and beyond to enable legally significant electronic transactions. An introduction to the project and its architecture for trustworthy global transactions is provided in Hühnlein [161].

5.4.1.3 Trustworthiness requirements defined in FutureTrust

Section 9 (pages 45 to 51) of *Deliverable 2.5 On Trust and Trust Models* [229] defines two types of requirements:

- requirements applicable to all participants, prior to an interaction;
- requirements applicable to participants interacting within the FutureTrust architecture in a specific role.

.

We next analyse the relevance of these requirements to this thesis.

5.4.2 Requirements applicable to all participants

Subsection 9.1 ([229] page 45) of *Deliverable 2.5 On Trust and Trust Models* defines six requirements that are applicable to all participants regardless of their role in the FutureTrust architecture. These requirements are referred to as 'contextual requirements'. They are

- CR1 Linkable identity,
- CR2 Competently acting in role,
- CR3 Fiduciary obligations/responsibilities,
- CR4 Governance and controls,
- CR5 Transparency, and
- CR6 Legal basis for legal effect.

We next briefly introduce each of these.

5.4.2.1 CR1 Linkable identity

Identity should be uniquely established for participants. Identity is defined here as a set of attributes that uniquely identify a participant. The actual set of attributes will depend on the nature of the participant (e.g. natural person, legal person or automaton) and on the use case. The established identity should be linkable to other instances ('linkable identity'), because the qualities that will have to be demonstrated need to be attributed to a specific participant for its claims to be trustworthy. Additional possible requirements are the support of pseudonyms and the ability to withstand Sybil attacks [75].

5.4.2.2 CR2 Competently acting in role

Participants need to demonstrate that they possess relevant competences when acting in a role. Qualifications are a common way to demonstrate this. Which competences, and hence which qualifications are required, depends on the use case and the level of calibration (introduced later in the FutureTrust deliverable, in Section 10.7.1). Participants may provide evidence regarding their possession of qualifications, or such evidence may be provided by a third party (attestor). Whether self-declared or attestor-declared evidence is required, should be configurable in a policy (specified in the rulebook, introduced later in the FutureTrust deliverable, in Section 10.4.1). It should also be possible to specify the independence of an attestor from the participant about whom the evidence is provided.

5.4.2.3 CR3 Fiduciary obligations/responsibilities

Actors may be subject to fiduciary obligations and responsibilities from law and regulations. They are also subject to less formal expectations of their responsibilities from consumers of their information or services. Actors should maintain a track record of having been demonstrably accountable, and having met their responsibilities and liabilities. This should include clear references to the applicable obligations/responsibilities.

5.4.2.4 CR4 Governance and controls

This requirement relates to having in place appropriate governance, security safeguards, and controls.

- Governance requires that accountability and responsibility is defined as well as communicated and accepted, and can be adjusted under a consensus model over time.
- Security safeguards require that appropriate technical security mechanisms are implemented and operated. This need is a consequence of the defined accountability and re-

sponsibility requirements, that necessitate principles such as integrity, access control, segregation of duty, 'four eyes', and limitations in time, to be maintained.

- Controls require that an entity that enforces or helps to enforce accountability and responsibility should be available to all participants. This includes the provision of assurance and of monitoring.

5.4.2.5 CR5 Transparency

Actors, their attestations and all other artefacts should be accessible to demonstrate sufficient transparency in order to allow verification of their claims by an interested party. Additionally, transparency helps to demonstrate that respect of third party rights is guaranteed.

5.4.2.6 CR6 Legal basis for legal effect

In those cases where legal effect is desired, a legal basis should be in place. This needs to be specified for each purpose. The purposes that need to be specified are varied and include electronic authentication, electronic signature, electronic seal, electronic preservation and electronic verification.

5.4.3 Requirements applicable to participants in a FutureTrust role

Deliverable 2.5 On Trust and Trust Models Subsection 9.2 ([229] page 49) defines requirements applicable to participants in a specific role within the FutureTrust architecture. These requirements are specified as 'use cases'. A description of the roles is given, followed by 27 role-specific use cases. Each use case includes a brief description, an identification of its actors, preconditions, main flow and postconditions. Required evidence is described for the preconditions, main flow and postconditions.

5.4.4 Using the FutureTrust trustworthiness requirements

Not all the Future Trust requirements are relevant here.Of the six categories described in Section 5.4.2, four are generally applicable. These are:

- CR1 Linkable identity,
- CR2 Competently acting in role,
- CR4 Governance and controls, and
- CR5 Transparency.

The other two categories focus on the legal value of services and their outputs. These are:

- CR3 Fiduciary obligations/responsibilities, and
- CR6 Legal basis for legal effect.

Taking the objectives of the thesis into account, the requirements in the four generally applicable categories (CR1, CR2, CR4, CR5) were used for the requirements of the $\mathcal{TE}$ model. The requirements in the two other categories (CR3, CR6) were not used as input because the legal value of trust services and their outputs falls outside the scope of the thesis.

The use cases described in Section 5.4.3 are FutureTrust-specific, including a focus on the legal value of evidence. Given the objectives of the thesis, the requirements in use cases were not used as input for the requirements of the $\mathcal{TE}$ model.

5.5 An integrated set of requirements

The SR-requirements derived from the literature survey and the four chosen CR-requirements from FutureTrust were combined into a single integrated set of requirements (IR-requirements) based on the analysis below. Figure 5.1 shows how the requirements were combined.

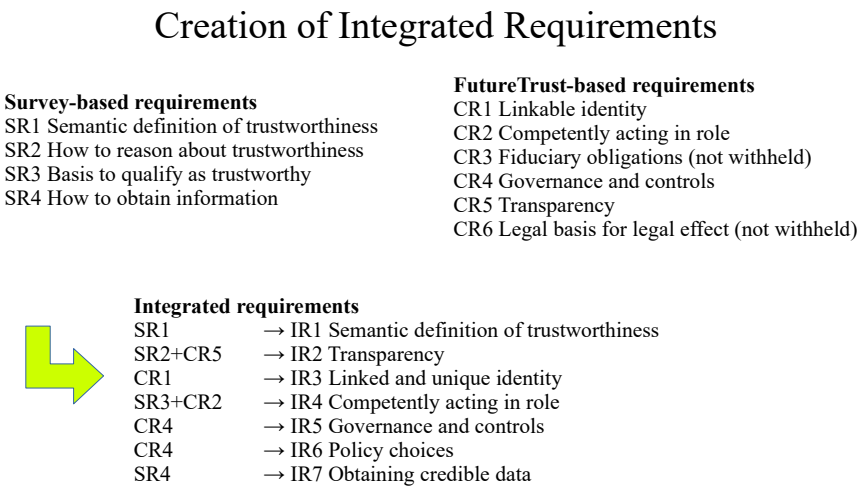

Figure 5.1: Combining the literature survey and FutureTrust requirements

The integrated requirements are specified in the following way:

- the initial context, described by the part *'As a participant'*,
- the action, described by the part *'I can'*, and
- the expected outcome, described by the part *'so that'*.

5.5.1 IR1 Semantic definition of trustworthiness

Survey requirement SR1 'Semantic definition of trustworthiness', defined in Section 5.3.1, is not related to any FutureTrust requirement. It is included without modification in the set of integrated requirements as requirement IR1 *Semantic definition of trustworthiness*, which is formulated as follows.

As a participant in an electronic ecosystem I can understand the meaning of trustworthiness of participants I plan to engage with, so that I can make an informed decision on whom to interact with.

5.5.2 IR2 Transparency

Survey requirement SR2 'How to reason about trustworthiness' defined in Section 5.3.2 is related to CR5 'Transparency' defined in Section 5.4.2.5. Since a possible participant in an electronic interaction must be able to understand the reasoning performed by a system that offers an evaluation of trustworthiness, the components that make up the system must be available. On this basis IR2 *Transparency* is as follows.

As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate trustworthiness of other participants, I can access all information (including inputs used and operations performed) of this function in a transparent[4] *way, so that I can understand the factors that contribute to trustworthiness and their mapping to evidence such as qualifications of entities.*

This implies:

- for 'inputs used':
  - definition of the factors of trustworthiness, and
  - mapping these inputs to understandable evidence such as qualifications of entities in well-defined semantics;
- for 'operations performed': the use of a deterministic and logic-based procedure.

5.5.3 IR3 Linked and unique identity

Integrated requirement IR3 is based on CR1 'Linkable identity' as defined in Section 5.4.2.1. Some observations regarding linkability are as follows.

[4]The term 'transparent' is used as defined in the Oxford English Dictionary figurative meaning, as 'frank, open, candid, ingenuous' and 'Easily seen through, recognized, understood, or detected; manifest, evident, obvious, clear.'

- Since information about participants is available from multiple sources, it must be possible to link all information pertaining to a particular participant to construct a set of information that can be used as input for the reasoning, i.e. it must be 'linkable'.
- It is not sufficient for the information to be linkable; to perform an evaluation of trustworthiness it must be correctly linked. Hence the requirement specifies 'linked' rather than 'linkable' unique identity.

Furthermore the CR1 requirement contains the statement 'Additional requirements are the support of pseudonyms, and the ability to withstand Sybil attacks.' Some further observations are as follows.

- While support for pseudonyms is relevant from the point of view of systems based on regulation, this requirement is not compatible with establishing a unique identity which would allow reasoning on the basis of all available information. Hence it is not a requirement for the model introduced in the next chapter.
- The ability to withstand Sybil attacks, as introduced by Douceur [74], is a specific requirement related to the creation of multiple identities, most relevant in a reputation system. However, reputation systems is not within the scope of the thesis, and hence this not a requirement for the model we develop.

This leads to the formulation of IR3 *Linked and unique identity* as follows.

As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate the trustworthiness of other participants, I can rely on this function combining all information about participants available within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation is based on all information known about the evaluated participant.

This implies:

- identity is defined as a set of attributes that uniquely identify a participant;
- all instances of the same identity must be linked because the qualities that will have to be demonstrated need to be attributed to a specific participant for the corresponding claims to be trustworthy.

5.5.4 IR4 Competently acting in role

There is a relation between requirement SR3, defined in Section 5.3.3, and requirement CR2 defined in Section 5.4.2.2. Because qualifications are a generally accepted way to demonstrate competence, integrated requirement IR4 *Competently acting in role* is as follows.

As a participant in an electronic ecosystem I have access to and I can demonstrate that I accept the definitions of roles, the qualifications that are required per role, and how these qualifications are demonstrated by participants, so that I can verify these arguments are suitable to support the reliance I want to take on the outcome of the reasoning.

5.5.5 IR5 Governance, security and controls

FutureTrust requirement CR4 'Governance and controls' defined in Section 5.4.2.4 is not related to any survey requirement. It is composed of three elements.

- Governance, which requires that accountability and responsibility is defined, communicated and accepted, and can be adjusted under a consensus model over time.
- Security safeguards, which require that mechanisms such as identification, authentication, access control, segregation of duty, limitations in time etc. are in place.
- Controls, which require that an entity that supervises participants in their roles must be in place and the results of its activities must be available to all participants. This includes the provision of assurance and monitoring.

This leads to integrated requirement IR5 *Governance and controls*.

As a participant in an electronic ecosystem I can understand the governance, security safeguards and controls that are in place within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation took into consideration that the ecosystem follows good practices regarding these topics.

5.5.6 IR6 Policy choices

We make a further observation regarding FutureTrust requirement CR4 'Governance and controls' defined in Section 5.4.2.4. There are many possible combinations of security safeguards and controls. Some combinations are more suitable to meet certain expectations than others. Seen from the point of view of a participant in an ecosystem it seems reasonable to require some degree of freedom regarding the choice of the combination most appropriate for the trustworthiness desired.

On this basis the integrated requirement IR6 *Policy choices* is as follows.

As a possible participant in an electronic interaction I can determine the information and the reasoning justifying that a participant is qualified as trustworthy, so that I can verify that information and reasoning are compatible with the way I want to rely on the outcome of the reasoning.

	Research Question	Addressed by
1	How can we semantically define trustworthiness?	IR1 Semantic definition of trustworthiness IR3 Linked and unique identity IR4 Competently acting in role IR5 Governance and controls IR6 Policy choices
2	How can we reason about trustworthiness?	IR2 Transparency IR7 Obtaining credible data
3	On what can reasoning to qualify an entity as trustworthy be based?	IR4 Competently acting in role IR7 Obtaining credible data
4	How can we obtain information for use in supporting such reasoning about 'real world' entities?	IR7 Obtaining credible data

Table 5.1: Research questions and integrated requirements

5.5.7 IR7 Obtaining credible data

Survey requirement SR4 'Information to reason about trustworthiness' defined in Section 5.3.4 is not related to any FutureTrust requirement. It is included without modification in the set of integrated requirements as requirement IR7 *Obtaining credible data* which is formulated as follows.

As a participant in an electronic ecosystem I can understand the origin and the type of data that is used in the evaluation of trustworthiness of participants, so that I can claim the outcome of the trustworthiness evaluation is based on credible data.

5.5.8 Relation to research questions

Table 5.1 illustrates how the research questions from Section 1.2.3 are addressed by the integrated requirements described in Section 5.5.

5.6 Summary

The objective of this chapter is to define requirements for a system to be defined and prototyped that supports the hypothesis given in Section 1.2.2, namely:

> *Where machine processable information about actors is available, it is desirable and possible to automate reasoning about the properties of these actors to support trust-related decision making based on formal semantics.*

These requirements are based on the findings from the literature survey described in Chapter 3 as well as on an elaboration of requirements developed by the author in the FutureTrust project[5]. A single set of integrated requirements was derived by merging these two sets.

As described in Section 5.3, the literature survey described in Chapter 3 identified four topics (SR1-SR4) relevant for further research. In Section 5.4, the requirements for trust and trustworthiness modelling developed in the FutureTrust project were analysed, and four of these requirements (CR1, CR2, CR3 and CR5) are relevant to this thesis. In Section 5.5, the four requirements derived from the literature survey and the four relevant requirements from FutureTrust were combined to give a single set of seven integrated requirements IR1-IR7. A mapping of the research questions from Section 1.2.3 against these seven requirements was also provided.

[5]http://www.futuretrust.eu

Chapter 6

Overview of the trustworthy ecosystem framework

This chapter presents an overview of the $\mathcal{TE}$ framework that forms the core of the work described in this thesis. It is intended to meet the requirements developed in the previous chapter.

6.1 Introduction

This chapter presents an overview of the trustworthy ecosystem ($\mathcal{TE}$) framework. Later chapters provide more details.

Section 6.2 identifies and analyses possible root causes for the lack of adequate semantics in trust-related decisions, and describes how the proposed $\mathcal{TE}$ framework addresses them. Section 6.3 provides the terminology used in the $\mathcal{TE}$ framework. Section 6.4 describes how the framework can be instantiated. Actors in the framework are situated in three planes, which are described in Section 6.5. Rulebooks are described in Section 6.6, and Section 6.7 covers the evaluation of trustworthiness. A summary is provided in Section 6.8.

6.2 Analysis of possible root causes

The digital society continues to increase its reliance on electronic representations of actors and the interactions they perform. Such interactions are conducted between entities which act as providers and consumers of services. Entities may be human users or digital agents. Relying on the outcome of an interaction performed via an ICT system, or selecting which system to use in the first place, forces an entity to take a trust-related decision.

We can identify two types of trust decision. Entities wishing to interact in the digital society

have firstly to select one or more other entities with which to interact. Secondly, after the interaction has taken place, they often have to respond to challenges regarding the trustworthiness of the interaction and its outcome. In both cases, there is a lack of a clear definition regarding the meaning of the information used as the basis for the trust decision, and the logic applied. We argue that the root causes for this lack include the points addressed in Section 6.2.1 immediately below.

6.2.1 The absence of well-defined semantics

The absence of well-defined semantics regarding trust and trustworthiness in prior art was identified as the first root cause. This was discussed in Section 3.5.3.1, and can be summarised as follows.

- There is a lack of consensus regarding whether trust is desirable in the first place.
- The trust frameworks and models that have been previously proposed are limited to a specific context or problem, and there is no general model that is commonly accepted as suitable.
- While PKI has been studied and deployed at large scale since the 1980s, and the term 'trusted third party' is commonly used, it is not clear what this term means. Huang [156] states that the major PKI specification documents do not precisely define what trust means in PKIs, and that there are implicit trust assumptions, some of which may not always be true. These implicit assumptions may cause relying parties to have differing understandings regarding the meaning of certificates and trust, which may possibly lead to a misuse of trust. Henderson [146] also argues that the semantics of trust in a PKI are not well defined.

Pretty Good Privacy (PGP) provides an alternative model of trust based on asynchronous distribution of public keys and certificates. In PGP, parties are represented by their public key; for a description see Blaze et al. [34], and for a review of the overall system state see Barenghi [22]. The PGP message format is described in RFC 4880 [42]. Certificates including public keys can be downloaded from public key servers[1]. Abdul-Rahman [2] describes the PGP trust model, where trustworthiness is explicitly defined in two ways.

- The trustworthiness of a public key certificate indicates whether one can be confident regarding the binding between the ID and public key contained in the certificate. This confidence is one of:

[1] From OpenPGP key servers such as `hkps://hkps.pool.sks-keyservers.net` or `http://pgp.mit.edu/` as well as from X.509 Directory Servers such as `keys.gnupg.net`

  - undefined,
  - marginal (the key may be valid but one cannot be sure), or
  - complete (one can be confident that this key is valid).

- The trustworthiness of an introducer indicates how much one can trust an entity represented by a public key to be a competent signer of another certificate. A user can assign four levels of trustworthiness:

  - full (this key is fully trusted to introduce another key),
  - marginal (this key can be trusted to introduce another public key, but it is not clear whether it is fully competent to do so),
  - untrustworthy (this key should not be trusted to introduce another), or
  - don't know (there are no expressions of trust made about this key).

The precise meaning of these trust levels is not defined explicitly. How the user arrives at an opinion about the introducer's trustworthiness is left up to the user. To allow flexibility and to cater for user-specific evaluation policies, PGP includes a tunable 'scepticism' level based on two parameters[2] that allows a user to define the minimum number of introducers required for a certificate to be deemed valid. The single scepticism level affects all of the keys in the user's keyring, so it is implicitly assumed that every key with the same trust level has exactly the same trustworthiness 'value'. Abdul-Rahman [2] gives the following criticism of this mechanism. The first problem is that these limited levels of trust are insufficient to reflect the highly varying opinions about trustworthiness that a user must put in a public key or introducer. Secondly, in real life each introducer will vary in their trustworthiness with respect to one another. However in PGP, given two marginally trusted introducers, one of them could be rated as twice as trustworthy as the other.

It thus appears that the meanings of trust levels for PGP are also not precisely defined, and the scepticism mechanism introduces implicit assumptions.

6.2.2 Reliance on simple hierarchical trust models

The reliance of trust-related reasoning in previous work on relatively simple hierarchical trust models, that are ill-suited to address the needs of a network of interacting agents, was identified as the second root cause. The following observations can be made.

- In Section 3.5.3.3 it was argued that, due to the continuous increasing diversification of service provision, the need for assurance about the quality of service delivery ranges from

[2] COMPLETES_NEEDED and MARGINALS_NEEDED

self-assurance to specialised third party assurance. Work by Mahmud [231] introduces trust factors such as 'security' but only defines them broadly, and neither is it specified precisely why and how such trust factors contribute to trust or trustworthiness.

- PKI is widely used as trust model for public key distribution. It is typically used in a hierarchical way, and trust in a CA public key means that all certificates signed by that CA are trusted. This provides a key management model for a range of applications including domain authentication in Transport Layer Security (TLS), mail authentication and code signing. This may be convenient for end users but does not allow users to gain a clear understanding of the basis for trust.

- PGP creates a graph of interrelationships by letting users sign keys they consider trustworthy, referred to as a web of trust[3]. However PGP lacks a mechanism to extend this graph with any other attributes. It also lacks a mechanism for propagating trust opinions within the PGP web of trust and introducer chains, or any form of trust-related chains. The graph of the web of trust is a fairly simple one, because is limited in depth and does not allow propagation of trust opinions.

6.2.3 Addressing these root causes

The trustworthy ecosystem framework proposed in this thesis addresses the issues discussed above in the following ways.

- Its data model is graph-based rather than hierarchical, allowing information from multiple sources to be combined in a corroborative way. A graph-based model enables effective evaluations of relationships between nodes. In such a graph, each node is identified by relating information (attributes) to it. In this way, information resides both in the edges and in the nodes, supporting logical reasoning.

- The framework explicitly specifies:

  - a data model that defines data points containing information about participants and their interactions,
  - a data import mechanism to create instance data according the data model,
  - a rulebook that lays down trustworthiness constraints on participants and their interactions, and

[3]The term 'web of trust' is also used for a reputation system created by the company WOT Services. The reputation system relies on user ratings and on third-party malware, phishing, scam and spam blacklists. This reputation system is unrelated to the PGP web of trust. There also exists a WOT ontology, available at `http://xmlns.com/wot/0.1/`. This ontology implements PKI concepts such as PubKey and EncryptedDocument.

  - trustworthiness evaluation algorithms which take as input:
    * a set of instance data, and
    * a rulebook.

The execution of a trustworthiness evaluation algorithm indicates whether constraints are satisfied on the basis of the available inputs. Satisfaction of the constraints contained in the rulebook is deemed to be a positive indication of trustworthiness.

The concept of a rulebook plays a central role in the proposed approach. Given the complexity of today's world, a single rulebook cannot be adequate for all types of electronic interactions between participants. The thesis presents one example of such a rulebook, based on the requirements from Section 5.2 and inspired by the eIDAS Regulation [103].

The data import mechanism imports real world data, referred to as instance data. How the data import mechanism is constructed is an implementation issue. A partial implementation of such a mechanism is described in Chapter 12.

The framework supports informed decisions on the basis of clear semantics, evidence and reasoning, based on an evaluation of trustworthiness. The integrated requirements elaborated in the previous chapter support such decision-taking. We recall these requirements are specified in the following way:

- the initial context, described by the part *'As a participant'*,
- the action, described by the part *'I can'*, and
- the expected outcome, described by the part *'so that'*.

The expected outcomes of the integrated requirements IR2 to IR7 contain arguments that support decision taking, since they are formulated as:

- *IR2 ..., so that I can understand the factors that contribute to trustworthiness and their mapping on evidence such as qualifications of entities.*
- *IR 3 ..., so that I can claim the outcome of the trustworthiness evaluation is based on all information known about the evaluated participant.*
- *IR4 ..., so that I can verify these arguments are suitable to support the reliance I want to take on the reasoning's outcome.*
- *IR5..., so that I can claim the outcome of the trustworthiness evaluation took into consideration the ecosystem meets good practices regarding these topics.*
- *IR6 ..., so that I can verify that information and reasoning are compatible with the way I want to rely on the reasoning's outcome.*

- *IR7 ..., so that I can verify that information and reasoning are compatible with the way I want to rely on the reasoning's outcome.*

The trustworthiness framework proposed in this thesis formalises a selected set of relationships and attributes of an electronic ecosystem and its participants, to allow reasoning over the trustworthiness of participants as well as their interactions. This enables automation of the interpretations of trust claims and their resulting effects. The term interpretation refers to a mathematically defined interpretation, corresponding to an assignment of meaning to the symbols of a formal language. The interpretation used is truth functional.

6.3 Terminology

We next give definitions of some fundamental terms.

- The trustworthy ecosystem ($\mathcal{TE}$) framework represents selective elements of the real world. Its purpose is to allow automated reasoning about the trustworthiness of those elements. The framework is composed of the following four building blocks.
  - The *data model* defines predicates representing interacting entities and their attributes, including roles the entities can assume, the interactions themselves, and related attestations, evidence and claims. A data model is proposed in Chapter 7.
  - *Rulebooks* contain formal rules specifying constraints that apply to the other elements of the ecosystem, satisfaction of which defines trustworthiness for a particular context. A rulebook functions as a norm that is well-defined and transparent. There may be many rulebooks. An approach to the creation of rulebooks and a specific rulebook example are proposed in Chapter 8. The example is based on the requirements defined in Chapter 5.
  - *Trustworthiness evaluation functions* verify whether constraints are satisfied using a specific rulebook and a specific set of instance data. There are two types of trustworthiness evaluation functions, ex-ante and ex-post. This is further addressed in Section 6.7. Only one rulebook and set of instance data can be taken into account during an evaluation. Both an approach to create trustworthiness evaluation functions and a specific example are proposed in Chapter 9.
  - *Instance data* contains information about a specific set of entities. Instance data can be retrieved from a variety of information sources. For the trustworthiness evaluation to be relevant, instance data must be selected that applies to the entities that are subject to evaluation. The framework is limited to working with instance data that can be used as positive evidence, i.e. evidence which would allow a target

role to be judged untrustworthy is not taken into account. The study of negative evidence is a possible topic for future research.

An approach to the creation of instance data is proposed in Chapter 12.

- The ecosystem's participants are an open group of distributed agents. Open here means that the membership of the set can change dynamically, and can be large. The participants can be heterogeneous.
- For *trust* the definition of Castelfranchi [46] is used, that 'trust is in fact a deficiency of control that expresses itself as a desire to progress despite the inability to control'.
- For *trustworthiness* the definition given in Section 5.2.2 is used, i.e. trustworthiness is a characteristic of an entity, with the following properties.
  - For participants, trustworthiness is based on evidence in the form of attestations. Such attestations can be provided by the participants about themselves, or provided by another participant.
  - For interactions between participants and for the results of such interactions, trustworthiness is based on evidence in the form of evidence records. Such evidence is created by trustworthiness service providers. They provide services that enrich information with authenticity, commitments or electronic signatures.
- *Base roles* indicate the primary role a participant plays in the ecosystem. Demonstrating the qualifications for a base role comes at a cost and may take some time. Therefore base roles are likely to be relatively stable over time. Participants are free to claim one or more base roles.
- *Situational roles* indicate a specific role a participant plays in a situation such as an interactive session, an information transfer or information storage. Therefore situational roles are, as indicated by their name, bound to a specific situation. Participants are free to claim any situational role. Base roles and situational roles can be combined. The framework as defined here is limited to base roles. The study of situational roles is a possible topic for future research.
- The participants in the ecosystem can be divided into three planes, described in detail in Sections 6.5.1 – 6.5.3:
  - the enabler plane,
  - the trustworthiness provision plane, and
  - the functional plane.

This is illustrated in Figure 6.1. Participants may invoke services provided by participants from any plane. The rulebook and trustworthiness evaluation functions $twseval_{AP}$ *and* $twseval_{AE}$ (see Section 6.7 and Chapter 9) are situated outside the planes, and are available to all participants.

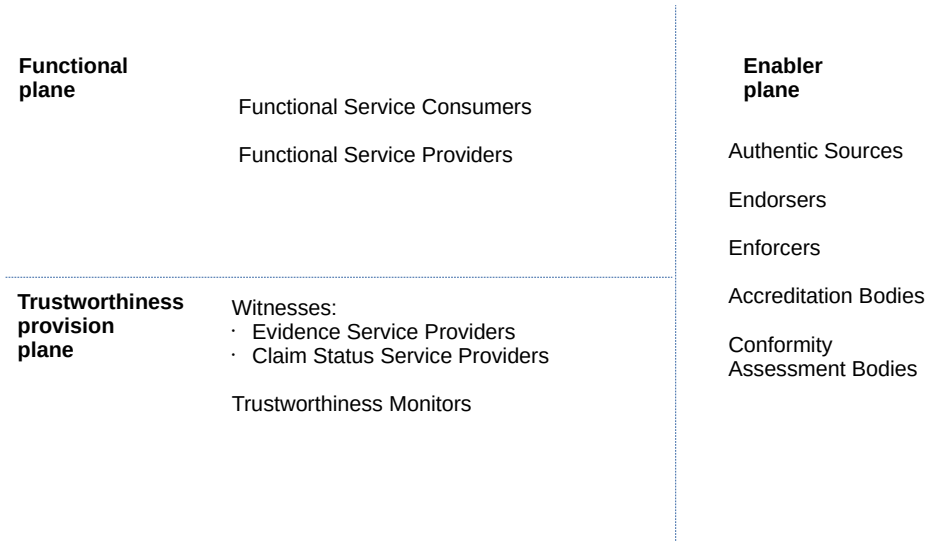

Figure 6.1: Base roles in the three planes

6.4 Instantiation

6.4.1 Overview

The framework specifications must be instantiated before they can be of practical use. This can be performed in the following way. The framework specifications consist of:

- the data model described in Chapter 7,
- a rulebook, such as the example described in Chapter 8,
- specifications for the evaluation of trustworthiness, such as those described in Chapter 9.

An instantiation of the framework is made by importing real world data, transformed according to the data model, into a suitable repository, and by creating queries that allow the satisfaction of the rules specified in the rulebook to be demonstrated. Technology has to be selected for this purpose. The use of a graph database for the repository together with SPARQL for formulating queries is proposed.

A function that evaluates trustworthiness takes as input a target ecosystem or a target participant, a set of rules from a rulebook and a set of instance data, and outputs either *true* or *false*.

- A function returns *true* when all of the evaluated rules return *true*. *True* means that the evaluated ecosystem or participant meets the constraints specified in the rules, which is an indication of trustworthiness.
- A function returns *false* when at least one of the evaluated rules return *false*. *False* means that the evaluated ecosystem or participant does not meets the constraints specified in the rules, which is an indication of a possible lack of trustworthiness.

6.4.2 Approach

One possible approach to developing a real-world instantiation of the framework is outlined below.

- One or more actors establish the ecosystem's rulebook and trustworthiness evaluation functions. For this purpose the predicates specified in the data model are used.
- At least one actor endorses the rulebook and, in doing so, takes on the role of an endorser.
- Actors are classified according to the data model on the basis of their attributes regarding identity and qualifications. Depending on the degree of desired trustworthiness:
  - these attributes must either be self-attested or attested by third parties,
  - these third parties must in turn be self-attested or attested by other third parties, and
  - additional attestations such as legal qualifications may be required.

Actors may also create a 'rulebook agreement' attestation to express their agreement to comply with the rules set-out in the rulebook and to respect the opinion of an enforcer.

The data import mechanism must be used to ensure the information in the model adequately reflects the situation of the real world.

6.5 Planes

As discussed above, the participants in the ecosystem are divided into three groups, referred to as planes.

6.5.1 The enabler plane

This plane forms the foundation of the ecosystem. The roles in this plane are as follows.

- Authentic Source (AS) role. An authentic source must hold a mandate to register and validate information about entities. This information, or part thereof, is then made available under its responsibility. The mandate can be a document that has legal validity because it is published in an official journal or because it is accepted to be binding through a contract or membership agreement. Competent authorities that allocate identifiers are examples of authentic sources. The purposes for these identifiers include trading, Value Added Tax collection and citizen identification (e.g. for the issue of passports, driving licences and identity cards).

- Endorser (EnDo) role. An endorser provides the applicable rules, legislation, and regulations and specifies who takes on responsibility, accountability, and authority to implement information security governance.

  An endorser expresses its publicly visible approval for this rulebook through its endorsement, and makes information on responsibility, accountability, and authority to implement information security governance available either itself or endorses information made available by another participant. Any participant can be an endorser.

- Enforcer (EnFo) role. An enforcer is an entity with power to enforce consequences among participants. An enforcer acts as arbiter or judge and provides the possibility for redress. Enforcement is outside the proposed system[4], but information about whether enforcement is available can be captured and reasoned about.

- The terminology of ISO/IEC 17000:2020 [173] is followed for the roles of Accreditation Body and Conformity Assessment Body. The standard defines conformity assessment as 'demonstration that specified requirements relating to a product, process, system, person, or body are fulfilled'. It defines 'specified requirement' as 'need or expectation that is stated'. The standard includes a note that states 'Specified requirements can be stated in normative documents such as regulations, standards and technical specifications.'

  - Accreditation Body (AB). An Accreditation Body is an entity that performs accreditation, i.e. the independent evaluation of conformity assessment bodies against

[4]One may evaluate the trustworthiness of a credit card provider in a variety of ways, for example that once all other possibilities are exhausted, potential disagreements will be settled before a court of law (an enforcer). Courts of law and all things legal are outside the credit card scheme. Nevertheless I can reason about whether the presence of such an enforcer improves the outcome of evaluation of trustworthiness. Marsh [234] Section 8.5 provides a detailed discussion of the role of an enforcer.

recognised criteria for their impartiality and competence. An AB accredits participants in the role of a Conformity Assessment Body. The United Kingdom Accreditation Service (UKAS) is an example of an entity in this role.

– Conformity Assessment Body (CAB) role. A CAB assesses the conformity of witnesses and their services against relevant criteria, and provides assurances of conformity in the form of attestations. In the UK, Lloyd's Register is an example of a CAB.

6.5.2 The trustworthiness provision plane

This plane involves participants that provide trustworthiness services. The principal roles in this plane are as follows.

- Witness roles. Witness roles provide attestations to facts, events or statements. We identify the following two special cases of witness roles.

  – Evidence Service Provider (EvSP) role. An EvSP creates information that serves as evidence. This name is proposed as a more generic alternative to the term Trust Service Provider. It includes traditional Trust Service Providers such as Certification Authorities, Identity Providers, Attribute Providers, (Remote) Signature Services, Time Stamp Services, and providers of added value services such as registered electronic delivery or archiving. Examples of well-known organisations in this role include Verisign[5] and Identrust[6].

  – Claim Status Service Provider (CsSP) role. A CsSP provides status information regarding claims, e.g. verifying a response to an authentication request, or verifying an electronic commitment or signature. Examples include the following.

    * In the public sector, the Belgian Federal Government offers a free eID Digital Signature Server[7]. It offers signature and verification services.
    * Private sector examples are the Belgian e-contract service[8] and Trustweaver's verification service[9] for electronic documents.

- Trustworthiness Monitor (TwsMo) role. A participant in this role monitors the provision of services by EvSPs and CsSPs and attests to this. Examples include the UK's tScheme and the Supervisory Bodies for the eIDAS Regulation [103] in the European Union.

[5] https://www.verisign.com/
[6] https://www.identrust.com/
[7] https://sign.belgium.be
[8] https://www.e-contract.be/dss
[9] https://twa.trustweaver.com/ap/validate.aspx

6.5.3 The functional plane

This plane consists of participants that act in the role of consumers or providers of a functional service. Prior to, during, and after service delivery these participants may invoke services from the other planes to evaluate the trustworthiness of participants. The principal roles in the functional plane are:

- Functional Service Providers (FuSPs), that offer business services, and
- Functional Service Consumers (FuSCs), that interact with FuSP services.

6.6 Rulebooks

A rulebook contains constraints in the form of rules which are used to determine whether an entity can be regarded as trustworthy. It contains mandatory rules whose satisfaction will always be verified, and discretionary rules which can be selected by the invoker of the trustworthiness evaluation function.

There may be many rulebooks. However, at the moment that a trustworthiness evaluation is performed, the rulebook that is to be taken into account must be specified. Only one rulebook can be taken into account during one evaluation. Rulebooks are described and an example is given in Chapter 8. Censi [47] provides an introduction to the use of rulebooks.

6.7 Trustworthiness evaluation

6.7.1 Introduction

Trustworthiness evaluation is defined as the conduct of a set of logical steps in which evidence is evaluated against a rulebook. Evidence in the form of a set of data points, represented according to the data model, is defined in Chapter 7. Rulebooks are addressed in Chapter 8, and how to perform the evaluation is described in Chapter 9. We now describe three fundamental aspects of trustworthiness evaluation and an approach to perform it.

6.7.2 Moment in time and scope

Trustworthiness evaluation can take place at various points in time.

- Prior to an interaction, a participant can choose from two ex-ante trustworthiness evaluation functions.

  - The ecosystem evaluation function ($twseval_{AE}$) can be invoked for assistance with a decision regarding whether to interact within a particular ecosystem, under a specific rulebook. An ecosystem can be qualified as ex-ante trustworthy upon satisfaction of the constraints of the trustworthiness evaluation policy specified by the trustor. This means that if a trustor decides to interact within the evaluated ecosystem, the trustor can have reasonable expectations that future interactions and their outcomes will be consistent with what has been described in the rulebook and endorsed by the endorser.
  - The participant evaluation function ($twseval_{AP}$) can be invoked for assistance with a decision regarding whether to interact with a particular participant. An entity can be qualified as ex-ante trustworthy upon satisfaction of the constraints of the trustworthiness evaluation policy specified by the trustor. This means that if a trustor decides to interact with the evaluated trustee, the trustor can have reasonable expectations that future interactions and their outcomes will be consistent with what has been communicated or committed by the trustee.

  The purpose of an ex-ante trustworthiness evaluation is to provide logical arguments to support trustor decision-making and provide supporting arguments should a choice be challenged. This type of evaluation forms the focus of much of the remainder of this thesis.

- During an interaction, a participant may invoke the trustworthiness provision services from a witness or a monitor. Functional interaction with invocation of trustworthiness services will lead to the creation of evidence, on which claims can be based. This part of the framework is not specified in detail in this thesis, and remains for future work (see Chapter 16).

- After an interaction, a participant may invoke the ex-post trustworthiness evaluation function ($twseval_{P}$) for assistance in deciding whether the outcome of the interaction with a particular participant can be deemed as trustworthy. The purpose of an ex-post trustworthiness evaluation is to support the trustor should the outcome of the transaction be challenged or rejected by another participant. Again, this part of the framework is not specified in detail in this thesis, and remains for future work (see Chapter 16).

6.7.3 Instance data

The $\mathcal{TE}$ framework allows the selection of a range of different information sources from which information can be used for trustworthiness evaluation. The sources must be identifiable and

trustworthy in their own right. This is addressed by selecting sources that are authoritative for the information they provide, as described in Chapter 10.

6.7.4 Execution capability

It is assumed that the party interested in the outcome of the trustworthiness evaluation function has direct access to and control over a device capable of executing the function. There may be cases where this is not possible due to a lack of resources or device constraints, or because the required instance data is not available to the interested party. In such cases it would be necessary to rely on another party to execute the function and return the results. However such cases are outside of the scope of the thesis and are topics for future research (see Chapter 16).

6.7.5 The four steps

The approach consists of four steps.

- The first step involves choosing whether to evaluate the trustworthiness of an ecosystem or a participant.
  - In the ecosystem case, the particular ecosystem and a specific rulebook are evaluated without specifying a particular participant.
  - In the participant case, a particular participant is evaluated as a potential trustee in the context of instance data and a rulebook.
- The second step involves selecting a rulebook and instance data. The rulebook β_I introduced in Chapter 8 is used as a working example in the discussions in this chapter. Selection of instance data is addressed in Chapter 10.
- The third step consists of selecting discretionary constraints from the rulebook that are relevant to the trustor's decision.
- The fourth step consists of executing the appropriate trustworthiness evaluation function to validate whether the mandatory and the selected discretionary constraints are satisfied by the selected instance data.
  - $twseval_{AE}$ is used when evaluating an ecosystem.
  - $twseval_{AP}$ is used when evaluating a specific participant as potential trustee.

6.8 Summary

This chapter identified and analysed the possible root causes for the lack of adequate semantics in trust-related decisions, and described how the $\mathcal{TE}$ framework addresses them. The terminology used in the framework was described. Ecosystem participants are divided into three planes, as listed below, where each plane contains participants acting in specified roles.

- The enabler plane, where participants in the roles of authentic source, endorser, enforcer, accreditation body and conformity assessment body are situated.
- The trustworthiness provision plane, where participants in the roles of evidence service provider, claim status service provider and trustworthiness monitor are situated.
- The functional plane, where participants in the roles of functional service provider and consumer are situated.

Rulebooks, which contain constraints in the form of rules, were described. They contain mandatory rules whose satisfaction will always be verified, and discretionary rules which can be selected by the invoker of the trustworthiness evaluation function for evaluation. Trustworthiness evaluation was defined as the conduct of a set of logical steps in which evidence is evaluated against a rulebook.

Chapter 7

Data model

This chapter presents the data model part of the $\mathcal{TE}$ framework. The data model is based on predicates. It includes predicates that represent interacting entities and their attributes, including roles they can assume. Predicates that represent interaction, evidence and claims are also included. Subsequent chapters describe how constraints are defined over the data, and how data and constraints are used to calculate trustworthiness.

7.1 Introduction

In this chapter the data model of the $\mathcal{TE}$ framework is defined. Data is represented by predicates which are selected on the basis of the requirements defined in Chapter 5. Subsequent chapters describe how constraints are defined over the data in the form of a set of rules (referred to as a 'rulebook'), and how trustworthiness can be calculated using the data and the constraints. An implementation of the data model is described in Chapter 11.

Section 7.2 describes the modelling of data points that contribute to meeting the requirements from Chapter 5, and how these data points are specified as predicates. The predicates *Actor*, *Attestations* and *Participants* are specified in Sections 7.3, 7.4 and 7.5. The base roles in which participants can act are specified in Section 7.6. Other attestations are specified in Sections 7.7 – 7.10. This includes *Agreement, Endorsement, Enforcement, Accreditation, Attestation of Conformance to a standard, Attestation of being under Monitor's supervision, Attestation of being registered, legal attestation and disclosure attestation.* Helper predicates are specified in Sections 7.11 and 7.12, and predicates for data sources are specified in Section 7.13. A summary is provided in Section 7.14.

7.2 Modelling the data

7.2.1 Meeting the requirements

7.2.1.1 Data points

Within the $\mathcal{TE}$ framework, data is made up of individual data points which are represented in the form of predicates. A data point is a unit of information which can be observed, analysed and processed. The purpose of data points in the $\mathcal{TE}$ framework is to serve as input to a trustworthiness evaluation function, which gives as output evidence to an ecosystem participant. This evidence is intended to give assurance to the participant that future interactions and their outcomes will be consistent with what has been communicated by the trustee, or that the outcome of a transaction performed in the past can be relied upon.

The data model has been designed to reflect the set of integrated requirements given in Section 5.5. Five of the seven requirements translate directly into elements of the data model, and these are listed immediately below.

- IR1 Semantic definition of trustworthiness. This is addressed by selecting data points that have a truth-functional interpretation.
- IR3 Linked and unique identity. To meet this requirement, data points capture various identity attributes. For this purpose the actor and participant predicates are created. This allows identity attributes to be related to entities.
- IR4 Competently acting in role. To meet this requirement, data points capture the role attributes specified per FLoC. For this purpose the role and attestation predicates are created. This allows roles and other attributes to be related to entities.
- IR5 Governance and controls. To meet this requirement, data points capture controls for integrity and authenticity. For this purpose the interaction, evidence and claim predicates are created. This allows interactions to be related to participants, and evidence/claims to be related to interactions, including the use of governance and control mechanisms.
- IR7 Obtaining credible data. To meet this requirement, selection criteria for data sources can be specified as data points. This is addressed in Section 12.1.

The remaining two requirements are addressed in the following ways.

- IR2 Transparency: this can be addressed by making all selected data points and their instantiation publicly available. However, this does not lead to the creation of a specific data point.

- IR6 Policy choices: this is addressed by selecting evaluation rules. This does not lead to the creation of a specific data point.

7.2.1.2 Predicates

As described above, predicates are used to model the data points that address requirements IR1, IR3, IR4, IR5 and IR7. The purpose of the predicates is to represent things from the real world so that they can be reasoned with.

A predicate has the form $Predicatename(term_1, term_2)$. When there is no need to specify a term's name it is represented by '_', such as in $Predicatename(term_1,\_)$

To refer to terms within a predicate, a projection function is used. It can be distinguished from the corresponding predicate by the use of a calligraphic letter in the first position. For example $Predicatename(term_1, term_2)$ is a predicate, and $\mathcal{P}redicatename(term_1, term_2)$ is a projection function. To improve readability the name of the projection function will include a subscript that refers to the term such as $\mathcal{P}redicatename_{term_1}(term_1, term_2)$.

The $\mathcal{TE}$ framework predicates are listed in Table 7.1, along with the part of this chapter in which they are described.

7.3 Actors

7.3.1 Purpose

The purpose of the actor predicate is to represent the class of things that are capable of acting in the real world. This allows reasoning about them in a trustworthiness evaluation.

7.3.2 Definition

An actor predicate represents the class of things from the real world that are capable of acting there. An actor is anything that can provide services to, or interact with, other actors, or is capable of reacting to stimuli from other actors within the $\mathcal{TE}$ framework. There are no constraints on who or what can be an actor. An actor predicate has the form $Actor(X)$. The set of all actors is denoted by S_A.

7.4 Attestations

7.4.1 Purpose

The purpose of the attestation predicate is to record attributes of actors. This allows reasoning about the presence, absence, or content of such qualities as part of trustworthiness reasoning

Predicate	**Reference**
Actor(X)	Section 7.3
Attestation(a_{id}, T) where a_{id} = the identity of the issuer of the attestation T ={*Subject, Attribute, Value*}	Section 7.4
Participant(X)	Section 7.5
Base role specified as *Attestation*(a_{id}, (*S, roleTypeBase, V*)	Section 7.6
Agreement specified as *Agreement*(a_{id},(*S, agreesTo, R*)	Section 7.7
Endorsement specified as *Endorsement*(a_{id}, (*S, doesEndorse, R*)	Section 7.8
Enforcement specified as *Enforcement*(a_{id}, (*S, doesEnforce, R*)	Section 7.9
Accreditation specified as *Accreditation*(a_{id}, (*S, accreditedFor, N*)	Section 7.10.1
Conformance to standard specified as *Conformance*(a_{id}, (*S, doesConformTo, V*)	Section 7.10.2
Supervision specified as *Supervision*(a_{id}, (*S, doesSupervise, V*)	Section 7.10.3
Registration specified as *Registration*(a_{id}, (*S, isRegisteredIn, R*)	Section 7.10.4
Legal qualification specified as *LegalQualification*(a_{id}, (*S, legalQual, V*)	Section 7.10.5
Disclosure attestation specified as *Disclosure*(a_{id}, (*S, doesDisclose, V*)	Section 7.10.6
Eco specified as *Eco*(E)	Section 7.11
TwsEco specified as *TwsEco*(E)	Section 7.12

Table 7.1: The $\mathcal{TE}$ framework predicates

about an actor.

7.4.2 Definition

An attestation predicate has the form $Attestation(a_{id}, T)$, where

- a_{id} represents the actor that issued the attestation, and
- T represents the triple (subject, attribute, value) where
  - *subject* identifies the actor that is the subject of the attestation,
  - *attribute* specifies the attribute that is attested by the issuer a_{id} about the subject, where attributes are defined as $S_{ag} = \{\text{seq } \mathbb{C}\}$, where $\mathbb{C}$ is the allowed characterset, and
  - *value* contains the value of the attribute.

The triple T is used to define identity attributes, role attributes and other attributes such as the agreement to respect the rules of the instantiation of the $\mathcal{TE}$ framework within which a participant is interacting. An actor can create attestations about itself or other participants.

An attestation predicate can be extended with time and commitment marks. For example the attestation $Attestation(p_{id}, T)$ can be extended with time and commitment marks to $Attestation(p_{id}, T, t_m, c_m)$. The set of all attestations is defined as S_{attn}.

7.4.3 Projection

The following projection functions are defined for the attestation predicate:

- $\mathcal{A}ttestation_{a_{id}}$(A) selects the issuer,
- other selections can be specified as follows.
  - $\mathcal{A}ttestation_{t_{sub}}$(A) selects the subject[1] of an attestation triple,
  - $\mathcal{A}ttestation_{t_{att}}$(A) selects the attribute type of an attestation triple, and
  - $\mathcal{A}ttestation_{t_{val}}$(A) selects the attribute value of an attestation triple.

[1] participants are identified by their eIdentifier, as specified in Section 7.5.3

7.4.4 Time, commitment and revocation

All attestations, as well as the predicates described in the subsequent sections, can be extended with time and commitment marks. For example

$$Attestation(a_{id}, T)$$

can be extended to

$$Attestation(a_{id}, T, t_m, c_m)$$

An issued attestation can at any time be revoked (i.e. rendered invalid) by its issuer, using time and commitment marks, as described below.

7.4.4.1 Time marks

A time mark t_m is an optional set of attributes that express time of creation (*cre*), start of validity (*sov*), and end of validity (*eov*). Its creation is handled by the commitment creation function described below.

7.4.4.2 Commitment marks

A commitment mark c_m is an optional attribute that expresses the commitment of its creator. The commitment creation lifecycle is as follows.

- Prior to creating a commitment the committing actor has to invoke a commitment preparation function $f_{comprep}(a_{id1})$. The function generates and returns two elements:
  - commitment creation data which is to be kept internal and is required to create a commitment,
  - commitment validation data of the form

$$CVD(a_{id1}, commitment\text{-}validation\text{-}data, data).$$

- To commit information, an actor invokes the commitment creation function

$$f_{comcreate}(a_{id}, P)$$

  which extends the predicate P with a time and commitment mark. The function has access to the actor's internal commitment creation data, and a timestamp function.

- To verify a commitment, an actor invokes a commitment verification function

$$f_{comverif}(\textit{Predicate, CVD}(a_{id1}, (a_{id2}, \textit{commitment-validation-data, data})))$$

  which verifies the predicate's time and commitment marks. It returns true if the verification was successful and false otherwise. The function has access to the creator's attestation that contains the commitment validation data.

Commitment can be based on an electronic signature or a commitment scheme. How it is implemented is outside of the scope of this thesis.

7.4.4.3 Revocation

Revocation is performed by creating a attestation of the same type and with the same content as the attestation to be revoked. This new attestation must have a more recent time of creation than the original attestation's time of creation, a validity period of zero, i.e. *(sov = eov)*, and a commitment mark c_m.

7.5 Participants

7.5.1 Purpose

The purpose of the participant predicate is to qualify actors that meet a minimum set of constraints. Actors that meet the minimum set of constraints are qualified as participants. The presence or absence of this qualification is verified as part of an actor's trustworthiness evaluation.

7.5.2 Definition

A participant predicate has the form *Participant*(*X*). A participant is an actor that:

- is uniquely identified,
- is either a natural person or an organisation, and
- agrees to comply to the constraints formulated in one or more rulebooks.

These three required characteristics are expressed through attestation predicates. The set of all participants is denoted by S_{PT}.

7.5.3 Participant identification

Identification is defined by requirement IR3 in Section 5.5.3.

As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate trustworthiness of other participants, I can rely on this function combining all information about participants available within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation is based on all information known about the evaluated participant.

We recall this implies:

- Identity is defined as a set of attributes that uniquely identify a participant.
- All instances of the same identity must be linked because the qualities that will have to be demonstrated need to be attributed to a specific participant for the corresponding claims to be trustworthy.

For participants, the $\mathcal{TE}$ data model is structured in two parts:

- the minimum $\mathcal{TE}$ data model, and
- the extended $\mathcal{TE}$ data model.

The minimum $\mathcal{TE}$ data model is deliberately simple. Each participant X is identified by its eIdentifier. This is a unique constant and $\forall$ X : f_{id}(X) = c.

Attributes are related to participants by attestations. Possible attribute values for participants are as follows.

- The attributes for identification of natural persons are S_{aip} = {eIdentifier, givenName, middleName, firstName, dateOfBirth}. A natural person must at least have an eIdentifier and a givenName.
- The attributes for identification of organisations are S_{aio} = {eIdentifier, orgName, dateOfEstablishment}. An organisation must at least have an eIdentifier and an orgName.

The responsibility for issuing eIdentifiers and names is outside the scope of this thesis.

Invoking the projection function for the identity attribute eIdentifier can be achieved

- by specifying the attribute $\mathcal{A}ttestation_{t_{att}}$(A) as eIdentifier and retrieving its corresponding $\mathcal{A}ttestation_{t_{val}}$(A), or
- directly via $\mathcal{A}ttestation_{t_{eIdentifier}}$(A).

The extended $\mathcal{TE}$ data model allows other attributes to be assigned to participants. For example:

- a social security number, or the name and date of birth of one or more parents could be included in a natural person attestation;
- the legal form and Value Added Tax number (or similar) could be included in an organisation attestation.

However, in this thesis we restrict our attention to the minimum data model.

7.6 Base roles

7.6.1 Purpose

The purpose of the base role predicate is to express that, according to its issuer, a participant meets the requirements to act in the role indicated by the predicate. The role is one of the base roles introduced in Section 6.5. As the rulebook contains constraints on participant attributes which are role-dependent, checking these constraints is part of a participant's trustworthiness evaluation.

7.6.2 Definition

The following base roles were introduced in Section 6.5.

- Enabler plane (defined in Section 6.5.1):
  - Authentic Source,
  - Endorser,
  - Enforcer,
  - Accreditation Body, and
  - Conformity Assessment Body.
- Trustworthiness provision plane (defined in Section 6.5.2):
  - Witness, including:
    - Evidence service provider,
    - Claim status service provider, and
  - Trustworthiness Monitor.
- Functional plane (specified in Section 6.5.3):
  - Functional service provider, and

- Functional service consumer.

The base roles are depicted in three planes in Figure 6.1.

7.6.3 Base roletype attributes

A base role predicate consists of an attestation with attribute *roleTypeBase*, specified as *Attestation*(a_{id}, (*S, roleTypeBase, V*).

- *S* represents the subject of the attestation, i.e. the participant that is attested with the base role specified by *V*.
- The attribute for the base roletype is defined as $S_{abr} = \{roleTypeBase\}$.
- Values are defined as $V = seq\ \mathbb{C}$ where

  $v \in S_{arb} = \{R_{FuSP}, R_{FuSC}, R_{EnDo}, R_{EnFo}, R_{AB}, R_{CAB}, R_{EvSP}, R_{CsSP}, R_{TwsMo}\}$

The set of base role attestations is denoted by S_{abr}, where $S_{abr} \subset S_{attn}$.

7.7 Agreement

7.7.1 Purpose

The purpose of an agreement is to capture the fact that a participant has agreed to comply with a specific rulebook. Such an agreement makes it clear that a participant accepts being evaluated according to the rules specified by the rulebook, and will respect the opinion of an enforcer.

7.7.2 Definition

An agreement has the form *Agreement*(a_{id}, *T*), where

- a_{id} denotes the actor that issued the agreement, and
- *T* denotes the triple (subject, attribute, value) where
  - *subject* denotes the actor that is the subject of the attestation,
  - *attribute* specifies the attribute that is attested by the issuer a_{id} about the subject, where the attribute is defined as *agreesTo*, and
  - *value* contains the value of the attribute, which is the rulebook identifier.

The set of agreements is denoted by S_{agr}.

7.8 Endorsement

7.8.1 Purpose

The purpose of an endorsement is to describe that a participant endorses a specific rulebook. In this way, the endorser expresses its approval for the rulebook in a way that is publicly visible.

7.8.2 Definition

An endorsement has the form *Endorsement*(a_{id}, (*S, doesEndorse, R*)) where

- a_{id} denotes the issuer,
- *S* denotes the subject (i.e. the participant that endorses), and
- *R* denotes the rulebook.

A trustworthy ecosystem must have exactly one endorsed[2] rulebook, because the rulebook contains the constraints that are the basis for trustworthiness evaluation. The set of endorsements is denoted by S_{end}.

7.9 Enforcement

7.9.1 Purpose

The purpose of an enforcement is to indicate that a participant is willing and able to enforce a rulebook[3]. Recall that an enforcer is an entity with power to enforce consequences among participants. While enforcement itself is external to the $\mathcal{TE}$ framework, the presence of an enforcer is part of trustworthiness evaluation.

7.9.2 Definition

An enforcement has the form *Enforcement*(a_{id}, (*S, doesEnforce, R*)) where

- a_{id} denotes the issuer,
- *S* denotes the subject (i.e. the participant that enforces), and

[2] It can be argued that it is sufficient to have agreement attestations from the individual participants, and that an endorsement is not required. Illustrations of this approach can be seen in so-called self-sovereign models. However, the framework is based on the integrated requirements given in Chapter 5, and IR5 'Governance, security and controls' leads to the need for endorsement.

[3] As for endorsement, the need for enforcement derives from requirement IR5 'Governance, security and controls'.

- R denotes the rulebook.

The set of enforcements is denoted by S_{Enf}.

7.10 Other attestations

7.10.1 Accreditation

7.10.1.1 Purpose

The purpose of an accreditation assertion is to indicate that a participant is accredited by an accreditation body to assess the conformity of another participant according to a specific norm. The need for accreditation derives from requirement IR5 'Governance, security and controls'. Recall that an accreditor, formally an Accreditation Body (AB), is a participant that performs accreditation, i.e. the independent evaluation of conformity assessment bodies against recognised criteria for their impartiality and competence. An AB accredits participants in the role of a Conformity Assessment Body. While accreditation itself is external to the $\mathcal{TE}$ framework, the presence of an accreditation body is part of trustworthiness evaluation.

7.10.1.2 Definition

An accreditation takes the form *Accreditation*(a_{id}, (*S, accreditedFor, N*)) where

- a_{id} denotes the issuer of the accreditation,
- S denotes the subject (i.e. the participant that has been accredited), and
- N denotes the norm.

The set of accreditations is denoted by S_{Acc}.

7.10.2 Conformance to standard

7.10.2.1 Purpose

The purpose of a conformance to standard assertion is to indicate that, according to a conformity assessment body, a participant complies with the standard specified in the attestation.

The need for conformance to standards derives from requirement IR5 'Governance, security and controls'. Recall that a Conformity Assessment Body (CAB) is an entity that verifies the conformity of witnesses and their services against relevant criteria, and provides assurances of conformity in the form of attestations. A CAB is qualified as such by an AB.

While conformity assessment itself is external to the $\mathcal{TE}$ framework, the presence of an attestation of conformance to standards is part of trustworthiness evaluation. This is based on the assumption that compliance to a standard is a commonly accepted way to demonstrate requirements are met. Obviously this does not stop a claimant from demonstrating requirements are met in another way. However, such alternative ways are outside the scope of the thesis.

7.10.2.2 Definition

An attestation of conformance to a standard consists of an attestation with attributetype *doesConformTo* whose value refers to the standard. It is specified as *Conformance*(a_{id}, (*S, doesConformTo, N*) where

- a_{id} denotes the issuer of the conformance assertion,
- S denotes the subject (i.e. the participant that has been conformity assessed), and
- N denotes the norm.

The set of conformity to standards attestations is denoted by S_{ctsa}.

7.10.3 Supervision

7.10.3.1 Purpose

The purpose of a supervision assertion is to indicate that a trustworthiness monitor[4] is supervising another participant. Recall that a trustworthiness monitor is an entity with the mandate to supervise the activities of participants that deliver trustworthiness services, such as evidence service providers and claim status service providers. While the supervision itself is external to the $\mathcal{TE}$ framework, the presence of a trustworthiness monitor that performs supervision is part of trustworthiness evaluation.

7.10.3.2 Definition

An attestation of supervision consists of an attestation with attributetype *doesSupervise*. It is specified as *Supervision*(a_{id}, (*S, doesSupervise, P*)) where

- a_{id} denotes the issuer of the supervision assertion,
- S denotes the subject (i.e. the participant that performs the supervision), and
- P denotes the participant that is being supervised.

The set of supervision attestations is denoted by S_{sup}.

[4]The need for supervision derives from requirement IR5 'Governance, security and controls'.

7.10.4 Registration

7.10.4.1 Purpose

The purpose of a registration assertion is to indicate that, according to a registrar, a participant is listed in the register referred to in the attestation.

The need for being registered derives from requirements IR4 'Competently acting in role' and IR5 'Governance, security and controls'.

While such registration itself is external to the $\mathcal{TE}$ framework, the presence of an attestation of being registered is part of trustworthiness evaluation. This is based on the assumption that such registration is a commonly accepted way to demonstrate requirements are met. Obviously this does not stop a claimant from demonstrating requirements are met in another way. However, such alternative ways are outside the scope of this thesis.

7.10.4.2 Definition

It is specified as *Registration*(a_{id}, (*S, isRegisteredIn, R*)).

- a_{id} denotes the issuer of the registration assertion,
- *S* denotes the subject (i.e. the participant that is registered), and
- *R* denotes the register where the subject is registered.

The set of registration attestations is denoted by S_{rega}.

7.10.5 Legal qualification

7.10.5.1 Purpose

The purpose of a legal qualification assertion is to indicate that a participant is qualified through a legal document. The need for a qualification through a legal document derives from requirements IR4 'Competently acting in role' and IR7 'Obtaining credible data'.

7.10.5.2 Definition

A legal qualification is specified as *LegalQualification*(a_{id}, (*S, legalQual, L*)) where

- a_{id} denotes the issuer of the legal qualification,
- *S* denotes the subject (i.e. the participant that is legally qualified), and
- *L* denotes the URI that resolves to the legal norm to which the subject is legally qualified.

The set of legal document attestations is denoted by S_{lq}. The detailed semantics of legal documents are outside the scope of this thesis.

7.10.6 Disclosure

7.10.6.1 Purpose

The purpose of a disclosure assertion is to indicate that a participant has made a specific set of information available[5].

7.10.6.2 Definition

A disclosure consists of an attestation with attributetype *doesDisclose*, whose value takes a universal resource identifier that refers to the disclosed information.

It is specified as *Disclosure*(a_{id}, (*S, doesDisclose, D*)) where

- a_{id} denotes the issuer of the disclosure,
- *S* denotes the subject (i.e. the participant that is performing the disclosure), and
- *D* denotes the URI that resolves to the disclosure document.

The set of disclosure assertions is denoted by S_{dc}. The detailed semantics of disclosure documents are outside the scope of this thesis.

7.11 Eco helper predicate

7.11.1 Purpose

The predicate *Eco()* specifies that a combination of information establishes what is referred to as an ecosystem. It refers to the set of information that represents an ecosystem as a whole.

The predicate represents an ecosystem by representing a set of actors and information about them in the form of attestations, evidence and claims, as well as a rulebook containing sets of constraints over the other elements and trustworthiness evaluation functions capable of verifying that these constraints are satisfied.

7.11.2 Definition

An ecosystem predicate has the form *Eco(E)*.

[5]The need for a disclosure attestation derives from requirement IR5 ‘Governance, safeguards and controls’.

7.12 TwsEco helper predicate

7.12.1 Purpose

The predicate *TwsEco()* expresses the fact that, when specific constraints are satisfied, an ecosystem is trustworthy. The predicate *TwsEco*(E) refers to the set of information that represents an ecosystem that satisfies all mandatory rules and is referred to as a trustworthy ecosystem. The purpose of this predicate is to represent an ecosystem that meets formally defined constraints.

7.12.2 Definition

A trustworthy ecosystem predicate has the form *TwsEco*(E). The variable E refers to a set which may contain elements from

- S_{β}, the set of rulebooks,
- S_{A}, the set of actors,
- S_{attn}, the set of attestations,
- S_{PT}, the set of participants,
- S_{agr}, the set of agreements,
- S_{ds}, the set of data sources,
- S_{end}, the set of endorsements,
- S_{enf}, the set of enforcements,
- S_{int}, the set of interactions,
- S_{cla}, the set of claims,
- $S_{TwsEval}$, the set of trustworthiness evaluation functions.

7.13 Data sources

7.13.1 Purpose

The trustworthiness evaluations proposed here are based on inference and queries, using the predicates defined in this chapter. The purpose of the data source predicate is to identify sources of information that allow variable occurrences in other predicates to be bound[6] to data that represents a situation that is of interest.

[6]Bound means that substitution may no longer take place.

7.13.2 Definition

A data source predicate has the form *DataSource*(a_{id}, *URI, howPublished*) where

- a_{id} denotes the responsible for the data source,
- *URI* denotes where the data source can be accessed, and
- *howPublished* denotes the activity performed by the responsible to make the data source available.

The set of all data sources is denoted by S_{ds}.

7.14 Summary

The objective of this chapter was to define the data model for the $\mathcal{TE}$ framework. This data model is based on predicates. Predicates that represent interacting entities and their attributes, including roles they can assume, were defined, as well as predicates that represent attestations, interaction, evidence and claims. A predicate to represent data sources was defined that allows binding of variable occurrences to data that represents a situation that is of interest. The purpose and definition of each predicate were given. Projection functions were defined that allow the selection of individual predicate terms.

Chapter 8

Rulebooks

This chapter introduces the Rulebook, i.e. a set of constraints that reflect a particular context for reasoning about trustworthiness. Whilst the notion of a rulebook is a general one, two particular instances of a rulebook are also described which have been derived from the requirements developed in Chapter 5.

8.1 Introduction

This chapter introduces the concept of a Rulebook, a set of constraints that reflect a particular context for reasoning about trustworthiness. The constraints are formalised as rules describing expected qualities of, and relationships between, participants in the ecosystem. Verifying whether these rules are satisfied allows evaluation of the trustworthiness of an entire ecosystem or of a participant in the ecosystem. *Rule verification is evaluated by trustworthiness evaluation functions, which are described in the next chapter.* Whilst the notion of a rulebook is a general one, two closely related specific rulebooks are also described which have been derived from the requirements developed in Chapter 5. Both rulebooks include sets of mandatory and discretionary rules

Section 8.2 provides an overview of the structure and use of rulebooks. Section 8.3 describes an approach for the creation of rulebooks. Sections 8.4 – 8.8 illustrate this approach through the creation of a specific rulebook for the evaluation of an ecosystem. After a brief introduction in Section 8.4, Sections 8.5 – 8.8 provide formally specified rules corresponding to the the integrated requirements specified in Section 5.5. In a similar way, sections 8.9 – 8.13 illustrate this approach through the creation of a specific rulebook for the evaluation of a participant in an ecosystem. A summary is provided in Section 8.14.

8.2 Modelling constraints in rules

8.2.1 Purpose

The purpose of a rulebook is to formally capture an understanding of what trustworthiness means in a particular context, in the form of constraints on data points. This, in turn, enables reasoning about trustworthiness to be performed using the input instance data, using the formalisms introduced in Chapters 6 and 7.

8.2.2 Defining rulebooks

Rulebooks are the third of the four $\mathcal{TE}$ framework building blocks specified in Section 6.3. The other building blocks are the data model, the trustworthiness evaluation functions and instance data.

There may be multiple rulebooks. The set of all rulebooks is denoted by S_β. Each rulebook R is identified by its rulebook identifier (rIdentifier) r. This is a unique constant and $\forall$ R : f_{id}(R) = r.

A rulebook consists of a set of rules that are expressed in FOL. As discussed in Section 8.3, a rulebook contains both mandatory and discretionary rules.

8.2.3 Rulebook verification

While there may be multiple rulebooks, a trustworthiness evaluation must be performed using a single rulebook and a specific set of instance data. In an evaluation, the mandatory rules of this rulebook will be always be checked, along with those discretionary rules supporting the type of trustworthiness required. Clearly, the set of discretionary rules to be used in an evaluation must be specified in advance.

8.3 Approach for rulebook creation

In principle, many approaches could be used to create a rulebook. The approach adopted here is described below. Key elements of the approach are described in greater detail in Sections 8.3.1 and 8.3.2.

- The rulebook must be based on a well-defined set of requirements. The specific rulebooks described later in this chapter build on the requirements defined in Chapter 5.
- The rulebook must be expressed in a well-defined terminology. The specific rulebooks described later in this chapter use the terminology described in Chapters 6 and 7.
- Requirements must be specified using FOL.

- Two types of rulebook are defined which differ in their objective:
  - rulebooks that contain rules for the $twseval_{AE}$ function, which evaluates the trustworthiness of an ecosystem, and
  - rulebooks that contain rules for the $twseval_{AP}$ function, which evaluates the trustworthiness of a participant.
- Two ruletypes are defined which differ in when and how they are evaluated.
  - Mandatory rules are always evaluated. They define the minimum conditions that a data instance must satisfy in order to be evaluated as trustworthy in the $\mathcal{TE}$ framework.
  - Discretionary rules can be evaluated at the discretion of the invoker. They allow a policy for trustworthiness evaluation to be expressed.

A trade-off is possible between specifying constraints as mandatory or discretionary for a given rulebook. By including more constraints in the mandatory set, the bar is raised for an ecosystem or a participant to be deemed as trustworthy. However, this comes at the cost of reducing options to express policy, because a constraint cannot appear in both the mandatory and in the discretionary set. The specific rulebooks used as illustration include only a small set of mandatory constraints to allow flexibility in the creation of policy.

8.3.1 Rule formulation

We strove to formulate the rules in FOL in a consistent way. Where possible, patterns of the following types were used.

- The implication connective $\rightarrow$ is used to express constraints. A conditional statement of the form $p \rightarrow q$ is used to express that p is a constraint that must be met for q to be true. For example a rule expressing a participant is an actor that meets constraints c_1 and c_2 is written as follows.

$$\forall(X)(Actor(X) \wedge (c_1(X) \wedge c_2(X)) \rightarrow Participant(X))$$

- Mandatory rules that apply to a set of data that represents an ecosystem can be constructed as follows.

$$\forall(E)\ (Eco(E) \wedge (constraints) \rightarrow TwsEco(E))$$

The '$\forall(E)$' is referred to as the head of the pattern, while the remainder is referred as the tail. The constraints in the tail refer to individual data points in instance data.

- Discretionary rules mostly follow one of the following two patterns.

$$\forall\, X \in S_{PT}\ \exists\ A_1,\, A_2 \in S_{abr}\ \text{(constraints)}$$

$$\exists\, X \in S_{PT}\ \exists\ A_1,\, A_2 \in S_{attn}\ \text{(constraints)}$$

However, in a few cases other patterns are used, e.g. to specify segregation of duty requirements.

8.3.2 Mandatory and discretionary rules

A rulebook contains mandatory and discretionary rules. A trustworthiness evaluation combines mandatory rules (which are by default executed) and discretionary rules (whose execution depends on them being selected by the invoker).

The purpose of the mandatory rules is to ensure there is enough information in the instance data to allow reasoning that can result in a decision. The set of discretionary rules allows the invoker to select those rules that express policy requirements.

- The mandatory rules check instance data and express the requirements that must be met for the available information to be deemed to represent a trustworthy ecosystem or participant. At the moment of trustworthiness evaluation, all mandatory rules of the selected rulebook are verified. Within the specific rulebooks described later in this chapter, mandatory rules are identified as $\beta_{IRm\text{-}Mn}$ where m refers to the requirement on which the rule is based, M corresponds to 'Mandatory', and n is a sequence number.

- The discretionary rules affect the way the trustworthiness evaluation deductions are drawn from the information inside the system. Information might be available that positively contributes to trustworthiness, or required information might be missing. Within the specific rulebooks described later in this chapter, discretionary rules are identified as $\beta_{IRm\text{-}Dn}$ where m refers to the requirement on which the rule is based, D corresponds to 'Discretionary' and n is a sequence number. The following sub-numbering is applied.

  - Rules that formulate constraints that are ecosystem-wide are labelled as $\beta_{IRm\text{-}D0n}$.
  - Rules that formulate constraints of information that is provided by a participant about itself (self-attestations) are labelled as $\beta_{IRm\text{-}D1n}$.
  - Rules that formulate constraints of information that is provided by another participant (other-attestations) are labelled as $\beta_{IRm\text{-}D2n}$.

– Rules that formulate constraints of information that is provided by another participant that is legally qualified for this information (legally qualified-attestations) are labelled $\beta_{IRm\text{-}D3n}$.

For example, rule IR3-D11 is the first discretionary rule of the 'self' category, and rule IR3-D22 is the second discretionary rule of the 'other' category.

8.3.3 Two specific rulebooks

8.3.3.1 Description

As an illustration of the approach described above, in the remainder of this chapter two specific examples of a rulebook, denoted by β_{AE} and β_{AP}, are presented. Both are based on the integrated requirements defined in Section 5.5.

We describe how each requirement is addressed by the set of rules in the rulebook. For requirements IR2 – IR5, explicit rules are specified in FOL, derived from the requirements. In the remainder of this chapter we list the rules making up two specific rulebooks.

- The rules for the first rulebook are introduced in Sections 8.5 – 8.8, classified according to which of the requirements in Section 5.5 were used to motivate their inclusion. The names of the discretionary rules in this rulebook end in '-AE'.
- The rules for the second rulebook are introduced in Sections 8.10 – 8.13. They are classified in the same way as the rules of the first rulebook. The names of the discretionary rules in this rulebook end in '-AP'.

8.3.3.2 Addressing IR1, IR6 and IR7

In the cases of requirements IR1, IR6 and IR7, where it is not possible to specify explicit rules, the requirements have been addressed in each rulebook in the same way, as follows.

IR1 Semantic definition of trustworthiness Requirement IR1 is as follows.

> *As a participant in an electronic ecosystem I can understand the meaning of trustworthiness of participants I plan to engage with, so that I can make an informed decision on whom to interact with.*

No specific rules correspond to this requirement; it is instead addressed by specifying the rules in FOL, using a formal taxonomy over data points that have a truth-functional interpretation[1].

[1] While FOL adds value by its truth-functional interpretation, the implementation described in Chapter 10 refines

IR6 Policy choices Requirement IR6 is as follows.

> *As a possible participant in an electronic interaction I can determine the information and the reasoning justifying that a participant is qualified as trustworthy, so that I can verify that information and reasoning are compatible with the way I want to rely on the reasoning's outcome.*

This is addressed by making rules either mandatory or discretionary. The mandatory set is kept minimal. Its purpose is to ensure there is enough information to allow reasoning that can result in decision. The discretionary set allows the invoker to select those rules that correspond best to its policy.

IR7 Obtaining credible data Requirement IR7 is as follows.

> *As a participant in an electronic ecosystem I can understand the origin and the type of data that is used in the evaluation of trustworthiness of participants, so that I can claim the outcome of the trustworthiness evaluation is based on credible data.*

This requirement applies to data points, and is addressed in Section 12.1.

8.4 A specific rulebook for ecosystem evaluation

The rulebook β_{AE} can serve as a basis for trustworthiness evaluation of an ecosystem in the setting of a $\mathcal{TE}$ framework instantiation, but obviously it can be extended with additional rules. For example, rules on specific security safeguards, such as the use of hardware that is conformity-assessed, as well as the demonstration of the well-functioning of governance or security management processes, could be envisaged.

8.5 IR2 Transparency

Requirement IR2 is as follows.

> *As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate trustworthiness of other participants, I can access all information (including inputs used and operations performed) of this function in a*

this by using ontologies from the Worldwide Web Consortium. This improves interpretation because the ontologies are written in OWL, which allows expression of fine-grained constraints and provides a simple interpretation in natural language.

transparent way, so that I can understand the factors that contribute to trustworthiness and their mapping on evidence such as qualifications of entities.

This is addressed:

- by making the data model, the rules and the trustworthiness evaluation functions publicly available,
- by using instance data from publicly available sources. As this is a matter of implementation it is addressed in Chapter 10.

Mandatory and discretionary rules were also derived from requirement IR2; details of the rules themselves are given below.

8.5.1 Mandatory rules

8.5.1.1 Rulebook-related rules

As rulebooks contain the constraints whose satisfaction is evaluated during trustworthiness evaluation:

- there must be at least one rulebook, because otherwise there is no basis for trustworthiness evaluation, and
- every rulebook must be uniquely identified, because otherwise participants cannot unambiguously refer to it.

To meet these requirements, the rules specified in Figure 8.1 are included in the rulebook.

$\beta_{IR2\text{-}M01}$	A trustworthy ecosystem must have at least one rulebook	$\forall(E)$ $(Eco(E)$ $\wedge \exists\ \beta \in S_\beta$ $\rightarrow TwsEco(E))$
$\beta_{IR2\text{-}M02}$	Every rulebook must be uniquely identified	$\forall(E)$ $(Eco(E)$ $\wedge (\forall\ \beta \in S_\beta\ (f_{id}(\beta) = c \rightarrow \exists! c \in \mathcal{R}))$ $\rightarrow TwsEco(E))$

Figure 8.1: IR2 rulebook-related mandatory rules

8.5.1.2 Participant-related rules

For participants to interact with each other in a transparent way it is required that a participant is an identifiable and addressable entity. To meet this requirement, the rule specified in Figure 8.2 is included in the rulebook.

$\beta_{IR2\text{-}M10}$	A participant is an actor that has a given name (for a natural person) or an organisation name (for an organisation)	$\forall(X)$ $(Actor(X)$ $\wedge$ $(\exists\, A \in S_{attn}\, (Attestation_{t_{sub}}(A) = X))$ $\wedge$ $(((Attestation_{t_{att}}(A) = givenName)$ $\wedge\, (Attestation_{t_{val}}(A) \neq \emptyset))$ $\vee\, ((Attestation_{t_{att}}(A) = orgName)$ $\wedge\, (Attestation_{t_{val}}(A) \neq \emptyset)))$ $\rightarrow Participant(X))$

Figure 8.2: IR2 participant-related mandatory rule

8.5.2 Discretionary rules

8.5.2.1 Enabler plane rules

The enabler plane, introduced in Section 6.5.1, includes the roles of endorser, enforcer, authentic source, accreditation body and conformity assessment body. To allow a potential trustor to evaluate the trustworthiness of a potential trustee, we optionally require at least one participant to be present in each role. This requirement is formalised by the rules in Table 8.1.

8.5.2.2 Trustworthiness provision plane

The trustworthiness provision plane, introduced in Section 6.5.2, includes the roles of evidence service provider, claim status service provider and trustworthiness monitor. To allow a potential trustor to evaluate the trustworthiness of a potential trustee in the setting of a $\mathcal{TE}$ framework instantiation, we optionally require at least one participant to be present in each role. This requirement is formalised by the rules in Table 8.2.

8.5.2.3 Functional plane

The functional plane, introduced in Section 6.5.3, includes the roles of functional service provider and functional service consumer. To allow a potential trustor to evaluate the trustworthiness of a potential trustee in the setting of a $\mathcal{TE}$ framework instantiation, we optionally require at least

one participant to be present in each role. This requirement is formalised by the rules in Table 8.3.

8.6 IR3 Linked and unique identity

Requirement IR3 is as follows.

> *As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate trustworthiness of other participants, I can rely on this function combining all information about participants available within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation is based on all information known about the evaluated participant.*

The requirement for linked and unique identification of a participant can be informally defined as follows.

- Identity is defined as a set of attributes that uniquely identify a participant.
- All instances of the same identity must be linked because the qualities that have to be demonstrated need to be attributed to a specific participant for the corresponding claims to be trustworthy.
- Every participant must have an identity attestation containing an eIdentifier.
- If identity attestations for actors A and B contain the same eIdentifier then actors A and B are deemed to be the same participant.

These observations lead to the rules specified in Sections 8.6.1 and 8.6.2.

8.6.1 A mandatory rule

The single mandatory rule $\beta_{IR3\text{-}M01}$ for linked and unique identity is specified in Table 8.4. It follows directly from requirement IR3 by stating that identity must be unique, i.e. it must be resolvable to a unique identifier.

8.6.2 Discretionary rules

Discretionary rules related to identity are proposed below. First the basis for expressing such rules is analysed, and subsequently the rules are given.

8.6.2.1 Basis for expressing IR3 discretionary rules

A range of approaches to describing the quality of identity proofing have been proposed by standardisation and regulatory bodies. Some of the most widely discussed are as follows.

- ISO/IEC TS 29003:2018 [180] defines three levels of identity proofing as follows.
  - Level 1 corresponds to low confidence in the claimed or asserted identity. The identity must be unique within the context, there is an assumption the identity exists, and the subject is assumed to be bound to the identity. The identifying attributes and the binding are accepted without any checks.
  - Level 2 corresponds to moderate confidence in the claimed or asserted identity. As for Level 1, identity must be unique within the context. Further it must be established with reasonable confidence that the identity exists by checking that identifying attributes exist in corroborative evidence, and that the subject has some binding to the identity. The latter must be checked using one factor.
  - Level 3 corresponds to high confidence in the claimed or asserted identity. As for level 1, identity must be unique within the context. Further it must be strongly established that the identity exists in authoritative evidence, and the subject has a strong binding to the identity. The latter must be checked using two or more factors.

- European Implementing Act EU 2015/1502 [105] for the eIDAS Regulation [103] defines three eIDAS-specific levels of identity assurance for cross-border recognition of identity. EU 2015/1502 [105] Recital (4) states that ISO/IEC 29115:2013 [181] has been taken into account, but that the content of the eIDAS Regulation [103] differs in relation to identity proofing and verification requirements. Also the Member State identity arrangements and tools are implemented in diverging ways. The annex of EU 2015/1502 [105] contains 'Technical specifications and procedures for assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme.'

- ISO/IEC 29115:2013 [181] defines an entity authentication framework which specifies four 'levels of entity authentication'. Each level corresponds to a specified degree of confidence in the processes leading up to and including the authentication process itself. The levels of entity authentication are:
  - 1 *Low*: Little or no confidence in the claimed or asserted identity;
  - 2 *Medium*: Some confidence in the claimed or asserted identity;
  - 3 *High*: High confidence in the claimed or asserted identity;
  - 4 *Very high*: Very high confidence in the claimed or asserted identity.

- The US NIST Special Publication 'Digital Identity Guidelines' [135] introduces three separate assurance levels for identity.
  - The Identity Assurance Level (IAL) addresses the robustness of the identity proofing process. It is subdivided into three levels (IAL1, IAL2 and IAL3).
  - The Authenticator Assurance Level (AAL) addresses the robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier. It is subdivided into three levels.
  - The Federation Assurance Level (FAL) addresses the robustness of the assertion protocol when using a federated approach to communicate authentication and attribute information (if applicable). It is subdivided into three levels.

ISO/IEC TS 29003:2018 appears to be the most suitable for use here, since it is directly relevant and is of general applicability. EU 2015/1502 is specific to the eIDAS regulation and the EU context. ISO/IEC 29115 is relevant, but focuses on authentication rather than identity proofing. The Identity Assurance Level of NIST SP-800-63-3 is highly relevant, but is oriented towards a US context.

The discretionary rules regarding attestation of the quality of identity proofing are therefore based on the definitions in ISO/IEC TS 29003:2018, and more precisely on the Levels of Identity Proofing. Additional rules based on the other approaches could be defined in an analogous way.

8.6.2.2 The rules

The following discretionary rules are derived from IR3.

- A single rule regarding self-attestation is specified in Table 8.5.
- Rules regarding other-attestations are specified in Table 8.6 and Table 8.7.
- Rules relating to identity attestation by legally qualified entities are given in Table 8.8 and Table 8.9.
- An extension to the second rule in Table 8.8 involving the additional requirement that the ISO/IEC TS 29003:2018 Level of Identity Proofing 3 must be specified by the evidence service provider is given in Table 8.10.

8.7 IR4 Competently acting in role

Requirement IR4 is as follows.

As a participant in an electronic ecosystem I have access to and I can demonstrate that I accept the definitions of roles, the qualifications that are required per role, and how these qualifications are demonstrated by participants so that I can verify these arguments are suitable to support the reliance I want to take on the outcome of the reasoning.

8.7.1 A mandatory rule

The single mandatory rule that a participant's base roles must be self-attested is specified in Table 8.11. It follows from requirement IR4 because it excludes the inconsistency that a participant denies having a particular role while other participants attest to it.

8.7.2 Discretionary rules

8.7.2.1 Role attestation

A rule specifying that for every role for which a participant has an attestation, at least one must be a role attestation, is given in Table 8.12.

There is no discretionary self-attested rule for role attestation because this is already contained in the mandatory rule $\beta_{IR4-M01}$.

8.7.2.2 Accreditation bodies

The single rule regarding accreditation bodies is specified in Table 8.13. Rule $\beta_{IR4\text{-}D022\text{-}AE}$ is based on the possibility of accreditation bodies being voluntarily assessed against ISO/IEC 17011 [174], which covers requirements for accreditation bodies. The rule specifies that if one wants to rely on the services of an accreditation body that has an ISO/IEC 17011 [174] attestation then there must be such an accreditation body and its attestation must be provided by a member of the International Attestation Forum (IAF).

8.7.2.3 Conformity assessment bodies

Rules regarding conformity assessment bodies are specified in Table 8.14.

- Rule $\beta_{IR4\text{-}D023\text{-}AE}$ is based on the operating practices of the ISO Committee for conformity assessment[2] (ISO/CASCO) which mandates ISO/IEC 17065 [176] attestation for conformity assessment bodies.

[2] `https://www.iso.org/resources-for-conformity-assessment.html`

- Rule $\beta_{IR4\text{-}D024\text{-}AE}$ is based on the operating practices of the European Accreditation co-operation mechanism[3](EA) which prescribes a specific attestation for trust service provider assessment based on the dedicated ETSI standard [88] for a conformity assessment body that assesses such service providers.

Note that while the organisation and responsibilities of the EA are regulated by law, the accreditation provided by EA does not have the power of law. Therefore such accreditations are treated here as attestations by others but not as attested to by a legally qualified other.

Alternative rules can be envisaged that rely on other conformity assessment standards from the ISO International Categorisation of Standards ICS 03.120.20, which covers product and company certification[4]. However, as the ETSI standard [88] focuses specifically on requirements for conformity assessment bodies assessing trust service providers which is more specific than the standards from ICS 03.120.202, such as ISO/IEC 27006 [178] which specifies 'general requirements for bodies providing audit and certification of information security management systems', the ETSI standard is preferred.

Alternative rules can be envisaged that rely on conformity assessment as prescribed by the CA/Browser Forum. However, as the CA/Browser Forum focusses mainly on securing the communication between a browser and a web server by putting trust in Certification Authorities and browser manufacturers, this model is less suitable for the objectives of the thesis and is therefore not further explored.

8.7.2.4 Evidence service providers

Rules regarding evidence service providers are specified in Table 8.15.

- Rule $\beta_{IR4\text{-}D025\text{-}AE}$ is based on the possibility of service providers being voluntarily assessed against ISO/IEC 27001 [177], which covers requirements for the existence and operation of an Information Security Management System.

- Rule $\beta_{IR4\text{-}D026\text{-}AE}$ is based on the possibility of oversight by a trustworthiness monitor over an evidence service provider.

- Rule $\beta_{IR4\text{-}D027A\text{-}AE}$ is based on the eIDAS definitions of and registration requirements for trust service providers. For a discussion of this topic see Section 2.2.3.1. The definitions[5]

[3]The European co-operation for Accreditation is a dedicated not-for-profit appointed in Regulation (EC) No 765/2008 to develop and maintain a multilateral agreement of mutual recognition, the EA MLA, based on a harmonized accreditation infrastructure; see `https://european-accreditation.org/`

[4]`https://www.iso.org/ics/03.120.20/x/`

[5]eIDAS [103] Art. 3 specifies that 'trust service provider' means a natural or a legal person that provides one or more trust services either as a qualified or as a non-qualified trust service provider; 'trust service' means an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and vali-

are taken from the eIDAS Regulation [103] and the applicable ETSI standard [89]. The registration is taken from the eIDAS List of Trusted Lists which is available in human readable format[6] and in machine readable format[7]. The rule specifies that if one wants to rely on the services of an evidence service provider that has an eIDAS TSP attestation then there must be such an evidence service provider and it must be listed in a European Trusted List by a trustworthiness monitor.

- Rule $\beta_{IR4\text{-}D027B\text{-}AE}$ is based on the eIDAS conformity assessment of trust service providers. For a discussion of this topic see Section 2.2.3.1. Demonstrating conformance to ETSI EN 319 403 [88] is a possible way of demonstrating compliance with the eIDAS Regulation [103] requirements regarding trust service providers.

8.7.2.5 Claim status service providers

Rules regarding claim status service provider are given in Table 8.16.

- Rule $\beta_{IR4\text{-}D028\text{-}AE}$ is based on the possibility of service providers being voluntarily assessed against ISO/IEC 27001 [177], which covers requirements for existence and operation of an Information Security Management System.

- Rule $\beta_{IR4\text{-}D029\text{-}AE}$ is based on the possibility of oversight by a trustworthiness monitor over claim status service provider.

- Rule $\beta_{IR4\text{-}D030\text{-}AE}$ is based on the eIDAS definitions of and registration requirements for trust service providers, and is defined analogously to Rule $\beta_{IR4\text{-}D027A}$.

8.7.2.6 Attestations by legally qualified others

Rules regarding attestations by legally qualified others are specified in Tables 8.17 and 8.18.

- Rules $\beta_{IR4\text{-}D301A\text{-}AE} - \beta_{IR4\text{-}D304B\text{-}AE}$ specify that participants in the roles of endorser, enforcer, authentic source, accreditation body, trustworthiness monitor and evidence service provider must be attested to by a legal act.

- Rule $\beta_{IR4\text{-}D305\text{-}AE}$ is based on the eIDAS requirement (eIDAS [103] Art. 17) that a Member State should designate an eIDAS Supervisory Body (trustworthiness monitor) and the current practice that this body is registered in a European Trusted List.

dation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services.

[6] `https://webgate.ec.europa.eu/tl-browser/\#/`

[7] `https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml`

8.8 IR5 Governance, safeguards and controls

Requirement IR5 is as follows.

> *As a participant in an electronic ecosystem I can understand the governance, security safeguards and controls that are in place within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation took into consideration that the ecosystem meets good practices regarding these topics.*

8.8.1 Foundation for IR5 rules

To meet requirement IR5, data points that capture governance principles, security safeguards and controls need to be validated. For this purpose rules are formulated on the basis of good practice for which the following sources have been considered:

- standards from by an official standards publishing organisation such as ISO and ETSI;
- legislation published by states;
- other published guidance and principles[8].

We restrict our attention here to the first two categories since there is no simple way of determining the extent to which other guidance and principles are accepted, and by whom. The $\mathcal{TE}$ framework allows other good practice principles to be included if desired, although agreement would be needed on means to demonstrate compliance.

8.8.2 Discretionary governance rules

8.8.2.1 Foundation for governance rules

Governance of the entire ecosystem is relevant to all parties at all times, since being a participant requires establishing one's identity and have supporting identity attestations. It may also be necessary to have an agreement attestation, capturing assent to interact under the ecosystem rules. This requirement is captured in the rules discussed below.

Governance is also relevant when a user is deciding whether to use a service provider Since this is service provider specific, it is addressed as part of the trustworthiness evaluation functions described in Chapter 9. Other areas of governance exist but are outside the scope of the $\mathcal{TE}$ framework.

[8]Examples include documents such as Internet Engineering Task Force (IETF) Request for Comments (RFCs), standards from the World Wide Web Consortium (W3C) and the OASIS consortium, the International Security Forum's (ISF) Standard of Good Practice for Information Security, publications from the Open Web Application Security Project (OWASP) and publications from the Information Systems Audit and Control Association (ISACA) such as their Control Objectives for IT (COBIT) series.

8.8.2.2 Governance information disclosure rules

As specified in Section 6.5.1, in the $\mathcal{TE}$ framework the endorser is responsible for the availability of information regarding who takes on responsibility, accountability, and authority to implement information security governance. The availability of this information[9] is used to formulate two discretionary rules in Table 8.19. Both rules are based on ISO/IEC 27014:2013 [179]. They differ in the qualification of the source of disclosure.

8.8.3 Discretionary security rules

8.8.3.1 Foundation for security safeguards rules

Security safeguards require that appropriate technical security mechanisms are implemented and operated. They are consequences of the need for accountability and responsibility, and require controls such as segregation of duty to be in place.

IR5 rules regarding security safeguards are based on the premise that, to avoid conflicts of interest, the entities that define what needs to be complied with must be different from the entities that verify and enforce this compliance. This concept was introduced in the eighteenth century by Montesqieu [23] who argued that the executive, legislative, and judicial functions of government should be assigned to different bodies, so that attempts by one branch of government to infringe on political liberty might be restrained by the other branches. In an information security policy setting this is supported by the concept of separation of duty, discussed by Clark and Wilson [60]. Separation of duty has been studied extensively[10] and continues to be embedded in legislation. For example the US Sarbanes-Oxley Act [321] Title V Section 501 on the treatment of securities analysts states '(3) to establish structural and institutional safeguards within registered brokers or dealers to assure that securities analysts are separated by appropriate informational partitions within the firm from the review, pressure, or oversight of those whose involvement in investment banking activities might potentially bias their judgement or supervision;'.

Many other security safeguards can be envisaged such as the use of hardware that is conformity assessed or the proper functioning of security management processes.

8.8.3.2 Separation of duty rules

Rules regarding separation of duty are specified in the following tables.

[9] The operation of the governance processes is outside scope of the trustworthiness evaluation. Nevertheless one can reason about whether the presence and the disclosure of information on this topic improves the outcome of evaluation of trustworthiness. The inclusion of the operation of government processes as part of the trustworthiness evaluation is a possible area for future research.

[10] See e.g. Gligor et al. [126], Jha et al. [187] and Basin et al. [25].

- The rules in Table 8.20 specify that the function of endorser of the rules that make up an ecosystem must be separated from the enforcer of these rules.
- The rules in Table 8.21 are stronger than the previous rules. They specify separation between all the functions within the enabler plane (endorser, enforcer, accreditation body and conformity assessment body).
- Table 8.22 specifies separation of the role of the trustworthiness monitor from the monitored roles, namely the evidence service provider and claims status service provider.

8.8.4 Controls

Controls require that an entity that enforces or helps to enforce accountability and responsibility should be available to all participants. This includes the provision of assurance and monitoring. Enforcement, assurance and monitoring are already covered by existing rules in the following ways.

- $\beta_{IR2\text{-}D01A\text{-}AE}$ specifies that an endorser must exist within the ecosystem.
- $\beta_{IR2\text{-}D01B\text{-}AE}$ specifies that an enforcer must exist within the ecosystem.
- $\beta_{IR2\text{-}D03\text{-}AE}$ specifies that an accreditation body must exist within the ecosystem. The role of such a body is to assess the conformance of conformity assessment bodies, and in this way provide assurance.
- $\beta_{IR2\text{-}D04\text{-}AE}$ specifies that a conformity assessment body must exist within the ecosystem. The role of such a body is to assess conformance against norms, and in this way provide assurance.
- $\beta_{IR2\text{-}D07\text{-}AE}$ specifies that a trustworthiness monitor must exist within the ecosystem.

8.9 A specific rulebook for participant evaluation

The rulebook β_{AP} can serve as a basis for trustworthiness evaluation of an ecosystem in the setting of a $\mathcal{TE}$ framework instantiation, but obviously it can be extended with additional rules. As is the case for β_{AE}, additional rules on specific security safeguards, such as the use of hardware that is conformity-assessed, as well as the demonstration of the well-functioning of governance or security management processes, could be envisaged.

8.10 IR2 Transparency

Requirement IR2 is as follows.

> *As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate trustworthiness of other participants, I can access all information (including inputs used and operations performed) of this function in a transparent way, so that I can understand the factors that contribute to trustworthiness and their mapping on evidence such as qualifications of entities.*

This is addressed:

- by making the data model, the rules and the trustworthiness evaluation functions publicly available,
- by using instance data from publicly available sources. As this is a matter of implementation it is addressed in Chapter 10.

Mandatory and discretionary rules were derived from requirement IR2; details of the rules themselves are given below.

8.10.1 Mandatory rules

8.10.1.1 Rulebook-related rules

To meet the rulebook-related requirements, the rules specified in Figure 8.1 are included in the rulebook.

8.10.1.2 Participant-related rules

For participants to interact with each other in a transparent way it is required that a participant is an identifiable and addressable entity. To meet this requirement, the rule specified in Table 8.2 is included in the rulebook.

8.10.2 Discretionary rules

For IR2 Transparency, there are no discretionary rules, because for the purpose of $twseval_{AP}$, transparency is addressed by the mandatory rules.

8.11 IR3 Linked and unique identity

Requirement IR3 is as follows.

> *As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate trustworthiness of other participants, I can rely on this function combining all information about participants available within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation is based on all information known about the evaluated participant.*

8.11.1 Mandatory rules

The single mandatory rule $\beta_{IR3\text{-}M01}$, specified in Table 8.4, is included.

8.11.2 Discretionary rules

These rules allow selection of a policy on what basis participant identity must be established.

For β_{AP}, the rules in Tables 8.5 – 8.10 can be applied with minor modifications, required for the following reasons.

- The rules in rulebook β_{AE} include $\forall\, X \in S_{PT}$ in the head of the rule, because the rules apply to all participants within the ecosystem. However, the rules of rulebook β_{AP} only cover a single participant.
- The rules in rulebook β_{AE} do not specify the identity of the potential trustee. However, the rules of rulebook β_{AP} only apply to the participant that was identified by the potential trustor as the potential trustee.

The modified rules are specified in Tables 8.23 – 8.28.

8.12 IR4 Competently acting in role

Requirement IR4 is as follows.

> *As a participant in an electronic ecosystem I have access to and I can demonstrate that I accept the definitions of roles, the qualifications that are required per role, and how these qualifications are demonstrated by participants so that I can verify these arguments are suitable to support the reliance I want to take on the outcome of the reasoning.*

8.12.1 A mandatory rule

The single mandatory rule that a participant's base roles must be self-attested, specified in Table 8.11, is included.

8.12.2 Discretionary rules

These rules allow selection of a policy for evaluating competence of a participant.

- An appropriately modified version of the rule given in Table 8.12, requiring attestation of roles by third parties, is given in Table 8.29.
- An analogous modification of the rule in Table 8.13 is given in Table 8.30.
- Similarly, participant-specific modifications of the rules in Tables 8.14 – 8.16 are given in Tables 8.31 – 8.33.
- Finally, rules regarding attestations by legally qualified others are given in Tables 8.34 – 8.36.

8.13 IR5 Governance, safeguards and controls

Requirement IR5 is as follows.

> *As a participant in an electronic ecosystem I can understand the governance, security safeguards and controls that are in place within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation took into consideration that the ecosystem meets good practices regarding these topics.*

8.13.1 Mandatory rules

There are no mandatory rules for IR5 in the rulebook β_{AP}.

8.13.2 Discretionary rules

The rules regarding agreement, endorsement and enforcement are given in Table 8.37. The rules regarding legal qualification of endorser and enforcer are specified in Table 8.38.Rules regarding separation of duty are specified in Tables 8.39 – 8.41.

8.14 Summary

This chapter described the role of the Rulebook, i.e. a set of constraints designed to enable decisions to made about trustworthiness.

The constraints are formalised as rules that describe expected qualities of data representing qualities and relationships between participants in the ecosystem. A distinction is made between mandatory and discretionary rules. Mandatory rules describe the constraints that must be satisfied to have the minimal basis for trustworthiness. Discretionary rules allow the evaluator to specify a trustworthiness evaluation policy by selecting discretionary constraints to match the context of the evaluation.

Two closely related example rulebooks were proposed, whose rules were derived from the integrated requirements described in Chapter 5. The proposed rulebooks are expressed in the terminology described in Chapters 6 and 7, using first order logic.

$\beta_{IR2\text{-}D01A\text{-}AE}$	A trustworthy ecosystem must contain at least one endorser	$\forall(E)$ $(Eco(E)$ $\wedge (\exists\, A \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = R_{EnDo}))$ $\rightarrow TwsEco(E))$
$\beta_{IR2\text{-}D01B\text{-}AE}$	A trustworthy ecosystem must contain at least one enforcer	$\forall(E)$ $(Eco(E)$ $\wedge (\exists\, A \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = R_{EnFo}))$ $\rightarrow TwsEco(X))$
$\beta_{IR2\text{-}D02\text{-}AE}$	A trustworthy ecosystem must contain at least one authentic source	$\forall(E)$ $(Eco(E)$ $\wedge (\exists\, A \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = R_{AS}))$ $\rightarrow TwsEco(E))$
$\beta_{IR2\text{-}D03\text{-}AE}$	A trustworthy ecosystem must contain at least one accreditation body	$\forall(E)$ $(Eco(E)$ $\wedge (\exists\, A \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = R_{AB}))$ $\rightarrow TwsEco(E))$
$\beta_{IR2\text{-}D04\text{-}AE}$	A trustworthy ecosystem must contain at least one conformity assessment body	$\forall(E)$ $(Eco(E)$ $\wedge (\exists\, A \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = R_{CAB}))$ $\rightarrow TwsEco(E))$

Table 8.1: IR2 enabler plane-related discretionary rules

$\beta_{IR2\text{-}D05\text{-}AE}$	A trustworthy ecosystem must contain at least one evidence service provider	$\forall(E)$ $(Eco(E)$ $\wedge (\exists\, A \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = R_{EvSP}))$ $\rightarrow TwsEco(E))$
$\beta_{IR2\text{-}D06\text{-}AE}$	A trustworthy ecosystem must contain at least one claim status service provider	$\forall(E)$ $(Eco(E)$ $\wedge (\exists\, A \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = R_{CsSP}))$ $\rightarrow TwsEco(E))$
$\beta_{IR2\text{-}D07\text{-}AE}$	A trustworthy ecosystem must contain at least one trustworthiness monitor	$\forall(E)$ $(Eco(E)$ $\wedge (\exists\, A \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = R_{TwsMo}))$ $\rightarrow TwsEco(E))$

Table 8.2: IR2 trustworthiness provision plane-related discretionary rules

$\beta_{IR2\text{-}D08\text{-}AE}$	A trustworthy ecosystem must contain at least one functional service provider	$\forall(E)$ $(Eco(E)$ $\wedge (\exists\, A \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = R_{FuSP}))$ $\rightarrow TwsEco(E))$
$\beta_{IR2\text{-}D09\text{-}AE}$	A trustworthy ecosystem must contain at least one functional service consumer	$\forall(E)$ $(Eco(E)$ $\wedge (\exists\, A \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = R_{FuSC}))$ $\rightarrow TwsEco(E))$

Table 8.3: IR2 functional plane-related discretionary rules

$\beta_{IR3\text{-}M01}$	A participant is an actor that is uniquely identified *Remark: recall that as introduced in Section 7.5.3, $f_{id}(X)$ returns the unique eIdentifier value for a participant. This value is denoted by c.*	$\forall(X)$ $(Actor(X)$ $\wedge (\forall A \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = X$ $\wedge \mathcal{A}ttestation_{t_{att}}(A) = eIdentifier$ $\wedge \mathcal{A}ttestation_{t_{val}}(A) = c)$ $\rightarrow \exists! c \in \mathcal{P})$ $\rightarrow Participant(X))$ Alternatively $\forall(X)$ $(Actor(X)$ $\wedge (\exists A_1, A_2 \in S_{attn}$ $((A_1 \neq A_2)$ $\wedge (\mathcal{A}ttestation_{t_{sub}}(A_1) = X$ $\wedge \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier)$ $\wedge (\mathcal{A}ttestation_{t_{sub}}(A_2) = X$ $\wedge \mathcal{A}ttestation_{t_{att}}(A_2) = eIdentifier)$ $\rightarrow (\mathcal{A}ttestation_{t_{val}}(A_1) = \mathcal{A}ttestation_{t_{val}}(A_2))$ $\rightarrow Participant(X))$

Table 8.4: IR3 linked and unique identity mandatory rule

$\beta_{IR3\text{-}D11\text{-}AE}$	A participant's identity must be self-attested	$\forall X \in S_{PT}\ \exists A \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge \mathcal{A}ttestation_{t_{att}}(A) = eIdentifier$ $\wedge \mathcal{A}ttestation_{t_{val}}(A) = f_{id}(X)$ $\wedge \mathcal{A}ttestation_{a_{id}}(A) = \mathcal{A}ttestation_{t_{sub}}(A))$

Table 8.5: IR3 linked and unique identity discretionary rule/self

$\beta_{IR3\text{-}D21\text{-}AE}$	For all participants there must at least one identity attestation that is not self-attested	$\forall X \in S_{PT} \exists A \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(X)$ $\wedge \mathcal{A}ttestation_{t_{att}}(A) = eIdentifier$ $\rightarrow \mathcal{A}ttestation_{a_{id}}(A) \neq \mathcal{A}ttestation_{t_{val}}(A))$
$\beta_{IR3\text{-}D22\text{-}AE}$	The identity of every participant must be attested to by at least one evidence service provider	$\forall X \in S_{PT} \exists A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(X)$ $\wedge \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP})$
$\beta_{IR3\text{-}D23\text{-}AE}$	The identity of every participant must be attested to by at least one evidence service provider whose role has been attested to by a trustworthiness monitor	$\forall X \in S_{PT} \exists A_1, A_2, A_3, \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(X)$ $\wedge \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$

Table 8.6: IR3 linked and unique identity discretionary rules

$\beta_{IR3\text{-}D24\text{-}AE}$	The identity of every participant must be attested to by at least one evidence service provider • whose role has been attested to by a trustworthiness monitor • who confirms that the identifying attributes exist in corroborative evidence and the binding between an applicant and an identity was checked using one factor prior enrolment (ISO/IEC 29003:2018 Level 2)	$\forall X \in S_{PT}\ \exists\ A_1, A_2, A_3, A_4 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) =$ *ISO-IEC-TS-29003:2018:Level2*)
$\beta_{IR3\text{-}D25\text{-}AE}$	The identity of every participant must be attested to by at least one evidence service provider • whose role has been attested to by a trustworthiness monitor • who confirms that the identifying attributes exist in corroborative evidence and the binding between an applicant and an identity was checked using one factor prior enrolment (ISO/IEC 29003:2018 Level 3)	$\forall X \in S_{PT}\ \exists\ A_1, A_2, A_3, A_4 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) =$ *ISO-IEC-TS-29003:2018:Level3*)

Table 8.7: IR3 linked and unique identity discretionary rules

$\beta_{IR3\text{-}D31\text{-}AE}$	The identity of every participant must be attested to by at least one evidence service provider who is legally attested in that role	$\forall X \in S_{PT}\ \exists\ A_1, A_2, A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = uri)$
$\beta_{IR3\text{-}D32\text{-}AE}$	The identity of every participant • must be attested to by at least one evidence service provider whose role has been attested to by a trustworthiness monitor, and • the evidence service provider and the trustworthiness monitor are legally attested in their respective roles	$\forall X \in S_{PT}\ \exists\ A_1, A_2, A_3, A_4, A_5 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_4) = uri$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_5) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) = uri)$

Table 8.8: IR3 linked and unique identity discretionary rules

$\beta_{IR3\text{-}D33\text{-}AE}$	The identity of every participant must be attested to by at least one evidence service provider • whose role has been attested to by a trustworthiness monitor • who confirms that the identifying attributes exist in corroborative evidence and the binding between an applicant and an identity was checked using one factor prior enrolment (ISO/IEC 29003:2018 Level 2), and there must be legal attestation for the evidence service provider and trustworthiness monitor in their respective roles.	$\forall X \in S_{PT}\ \exists\ A_1, A_2, A_3, A_4, A_5, A_6 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_4) =$ $ISO\text{-}IEC\text{-}TS\text{-}29003\text{:}2018\text{:}Level2$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_5) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) = uri$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_6) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_6) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_6) = uri)$

Table 8.9: IR3 linked and unique identity discretionary rules

$\beta_{IR3\text{-}D34\text{-}AE}$	The identity of every participant must be attested to by at least one evidence service provider • whose role has been attested to by a trustworthiness monitor • who confirms that the identifying attributes exist in corroborative evidence and the binding between an applicant and an identity was checked using one factor prior enrolment (ISO/IEC 29003:2018 Level 3), and there must be legal attestation for the evidence service provider and trustworthiness monitor in their respective roles.	$\forall X \in S_{PT}\ \exists\ A_1, A_2, A_3, A_4, A_5, A_6 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_4) =$ *ISO-IEC-TS-29003:2018:Level3* $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_5) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) = uri$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_6) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_6) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_6) = uri)$

Table 8.10: IR3 linked and unique identity discretionary rules

$\beta_{IR4-M01}$	A participant's base roles must be self-attested	$\forall X \in S_{PT}\ \exists\ A_1, A_2 \in S_{abr}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = \mathcal{A}ttestation_{t_{val}}(A_1))$

Table 8.11: IR4 Mandatory rule

$\beta_{IR4\text{-}D021\text{-}AE}$	For each role that participants have attestations for, there must be at least one role attestation that is not self-attested	$\forall X \in S_{PT}\ \exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = \mathcal{A}ttestation_{t_{val}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) \neq \mathcal{A}ttestation_{a_{id}}(A_1))$

Table 8.12: IR4 Discretionary rules/others

$\beta_{IR4\text{-}D022\text{-}AE}$	Should one want to rely on the services of an accreditation body that has an ISO/IEC 17011 [174] attestation then there must be such an accreditation body and its attestation must be provided by a member of the International Attestation Forum (IAF)	$\exists\, X \in S_{PT}\ \exists\, A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{AB}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = ISO\text{-}IEC\text{-}17011{:}2017$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) \in \{IAF\text{-}Memberlist\})$

Table 8.13: IR4 Discretionary rules/AB

$\beta_{IR4\text{-}D023\text{-}AE}$	Should one want to rely on a conformity assessment body that has an ISO/IEC 17065 [176] attestation for the assessment of evidence or claim status service providers then there must be a conformity assessment body that has such attestation issued by a member of the EA	$\exists\, X \in S_{PT}\ \exists\, A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{CAB}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = ISO\text{-}IEC\text{-}17065{:}2012$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) \in \{EA\text{-}Memberlist\})$
$\beta_{IR4\text{-}D024\text{-}AE}$	Should one want to rely on a conformity assessment body that has an ETSI EN 319 403 [88] attestation for the assessment of evidence or claim status service providers then there must be a conformity assessment body that has such attestation issued by a member of the EA	$\exists\, X \in S_{PT}\ \exists\, A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{CAB}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = EN319403$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) \in \{EA\text{-}Memberlist\})$

Table 8.14: IR4 Discretionary rules/others/CAB

$\beta_{IR4\text{-}D025\text{-}AE}$	Should one want to rely on the services of an evidence service provider that has an ISO/IEC 27001 [177] attestation then there must be such an evidence service provider and its attestation must be provided by a member of the EA	$\exists\, X \in S_{PT}\ \exists\, A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = ISO\text{-}IEC\text{-}27001{:}2013$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) \in \{EA\text{-}Memberlist\})$
$\beta_{IR4-D026-AE}$	Should one want to rely on the services of an evidence service provider then there must be such an evidence service provider and it must be whose role has been attested to by a trustworthiness monitor	$\exists\, X \in S_{PT}\ \exists\, A_1 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EvSP}$ $\rightarrow \exists\, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{a_{id}}(A_1) = \mathcal{A}ttestation_{t_{sub}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{TwsMo}))$
$\beta_{IR4\text{-}D027A\text{-}AE}$	Should one want to rely on the services of an evidence service provider that has an eIDAS TSP attestation then there must be such an evidence service provider and it must be listed in a European Trusted List by a trustworthiness monitor	$\exists\, X \in S_{PT}\ \exists\, A_1, A_2, A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = isRegisteredIn$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = eIDASTrustList$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo})$
$\beta_{IR4\text{-}D027B\text{-}AE}$	Should one want to rely on the services of an evidence service provider that has an eIDAS TSP attestation then there must be such an evidence service provider and it must demonstrate conformance to ETSI EN 319 403 [87]	$\exists\, X \in S_{PT}\ \exists\, A_1, A_2, A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = ETSI\text{-}EN\text{-}319\text{-}403$

Table 8.15: IR4 Discretionary rules/others/EvSP

$\beta_{IR4\text{-}D028\text{-}AE}$	Should one want to rely on the services of a claim status service provider that has an ISO/IEC 27001 [177] attestation then there must be such a claim status service provider and its attestation must be provided by a member of the EA	$\exists\, X \in S_{PT}\ \exists\, A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{CsSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = ISO\text{-}IEC\text{-}27001{:}2013$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2)\ in\ \{EA\text{-}Memberlist\})$
$\beta_{IR4\text{-}D029\text{-}AE}$	Should one want to rely on the services of a claim status service provider then there must be such a claim status service provider and it must be whose role has been attested to by a trustworthiness monitor	$\exists\, X \in S_{PT}\ \exists\, A_1 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{CsSP}$ $\rightarrow \exists\, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{a_{id}}(A_1) = \mathcal{A}ttestation_{t_{sub}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{TwsMo}))$
$\beta_{IR4\text{-}D030\text{-}AE}$	Should one want to rely on the services of an claim status service provider that has an eIDAS TSP attestation then there must be such an claim status service provider and it must be listed in a European Trusted List by a trustworthiness monitor	$\exists\, X \in S_{PT}\ \exists\, A_1, A_2, A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{CsSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = isRegisteredIn$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = eIDASTrustList$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo})$

Table 8.16: IR4 Discretionary rules/others/CsSP

$\beta_{IR4\text{-}D301A\text{-}AE}$	Participants in the role of endorser must have a legally qualified attestation	$\forall X \in S_{PT}\ \exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnDo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(PT)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = uri)$
$\beta_{IR4\text{-}D301B\text{-}AE}$	Participants in the role of enforcer must have a legally qualified attestation	$\forall X \in S_{PT}\ \exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnFo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = uri)$
$\beta_{IR4\text{-}D302\text{-}AE}$	Participants in the role of authentic source must have a legally qualified attestation	$\forall X \in S_{PT}\ \exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{AS}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = uri)$
$\beta_{IR4\text{-}D303\text{-}AE}$	Participants in the role of accreditation body must have a legally qualified attestation	$\forall X \in S_{PT}\ \exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{AB}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = uri)$

Table 8.17: IR4 Discretionary rules/legal qualifications

$\beta_{IR4\text{-}D304A\text{-}AE}$	Participants in the role of trustworthiness monitor must have a legally qualified attestation	$\forall X \in S_{PT}\ \exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = uri)$
$\beta_{IR4\text{-}D304B\text{-}AE}$	Participants in the role of evidence service provider must have a legally qualified attestation	$\forall X \in S_{PT}\ \exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = uri)$
$\beta_{IR4\text{-}D305\text{-}AE}$	Participants in the role of an eIDAS trustworthiness monitor (Supervisory Body) must be registered in a European trusted list	$\forall X \in S_{PT}\ \exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = eIDAS\_Supervisory\_Body$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = uri)$

Table 8.18: IR4 Discretionary rules/legal qualifications

$\beta_{IR5\text{-}D01\text{-}AE}$	There exists an endorser who discloses information of who takes on responsibility, accountability, and authority for implementing information security governance in a self-attested attestation	$\exists\, X \in S_{PT}\ \exists\, A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnDo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_1) = \mathcal{A}ttestation_{t_{sub}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_2))$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesDisclose$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = uri)$
$\beta_{IR5\text{-}D02\text{-}AE}$	There exists a legally qualified endorser who discloses information of who takes on responsibility, accountability, and authority for implementing information security governance	$\exists\, X \in S_{PT}\ \exists\, A_1, A_2, A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnDo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_1) = \mathcal{A}ttestation_{t_{sub}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesDisclose$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = uri$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = uri)$

Table 8.19: IR5 governance disclosure discretionary rules

$\beta_{IR5\text{-}D11\text{-}AE}$	An endorser cannot be an enforcer	$\forall\, A_1 \in S_{attn}\ \forall\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnDo}$ $\rightarrow \nexists\, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EnFo}))$
$\beta_{IR5\text{-}D12\text{-}AE}$	An enforcer cannot be an endorser	$\forall\, A_1 \in S_{attn}\ \forall\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnFo}$ $\rightarrow \nexists\, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EnDo}))$

Table 8.20: IR5 discretionary rules regarding mutual exclusion of endorser and enforcer

$\beta_{IR5\text{-}D21\text{-}AE}$	Helper rule that defines the separation of duties in the enabler plane	$S_{SOD_1} = \{R_{EnDo}, R_{EnFo}, R_{AB}, R_{CAB}\}$
$\beta_{IR5\text{-}D22\text{-}AE}$	If participant is in S_{SOD_1} then only one role is allowed	$\forall\, A_1 \in S_{attn}\ \exists\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) \in S_{SOD_1}$ $\rightarrow \neg\ \exists\, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) \in S_{SOD_1}\ ))$

Table 8.21: IR5 discretionary rules regarding separation of duty for the enabler plane

$\beta_{IR5-D23-AE}$	Separation of duties for the trustworthiness monitor role	$\forall\, A_1 \in S_{attn}\ \forall\, X \in S_{PT}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{TwsMo}$ $\rightarrow \nexists\, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ (\mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\vee\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{CsSP})))$

Table 8.22: IR5 discretionary rule regarding separation of duty for the trustworthiness monitor role

$\beta_{IR3\text{-}D11\text{-}AP}$	The selected participant's identity must be self-attested	$\exists\, A \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A) = \mathcal{A}ttestation_{t_{sub}}(A))$

Table 8.23: IR3 linked and unique identity discretionary rule/self

$\beta_{IR3\text{-}D21\text{-}AP}$	For the selected participant there must at least one identity attestation that is not self-attested	$\exists\, A \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(P_l)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A) = eIdentifier$ $\rightarrow \mathcal{A}ttestation_{a_{id}}(A) \neq \mathcal{A}ttestation_{t_{val}}(A))$
$\beta_{IR3\text{-}D22\text{-}AP}$	The identity of the selected participant must be attested to by at least one evidence service provider	$\exists\, A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(P_l)$ $\wedge\, \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP})$
$\beta_{IR3\text{-}D23\text{-}AP}$	The identity of the selected participant must be attested to by at least one evidence service provider whose role has been attested to by a trustworthiness monitor	$\exists\, A_1, A_2, A_3, \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(P_l)$ $\wedge\, \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\, \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$

Table 8.24: IR3 linked and unique identity discretionary rules

$\beta_{IR3\text{-}D24\text{-}AP}$	The identity of the selected participant must be attested to by at least one evidence service provider • whose role has been attested to by a trustworthiness monitor • who confirms that the identifying attributes exist in corroborative evidence and the binding between an applicant and an identity was checked using one factor prior enrolment (ISO/IEC TS 29003:2018 Level 2)	$\exists\ A_1, A_2, A_3, A_4, A_5 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) =$ *ISO-IEC-TS-29003:2018:Level2*)
$\beta_{IR3\text{-}D25\text{-}AP}$	The identity of the selected participant must be attested to by at least one evidence service provider • whose role has been attested to by a trustworthiness monitor • who confirms that the identifying attributes exist in corroborative evidence and the binding between an applicant and an identity was checked using one factor prior enrolment (ISO/IEC TS 29003:2018 Level 3)	$\exists\ A_1, A_2, A_3, A_4, A_5 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) =$ *ISO-IEC-TS-29003:2018:Level3*)

Table 8.25: IR3 linked and unique identity discretionary rules

$\beta_{IR3\text{-}D31\text{-}AP}$	The identity of the selected participant must be attested to by at least one evidence service provider who is legally attested in that role	$\exists\ A_1, A_2, A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = uri)$
$\beta_{IR3\text{-}D32\text{-}AP}$	The identity of the selected participant • must be attested to by at least one evidence service provider whose role has been attested to by a trustworthiness monitor, and • the evidence service provider and the trustworthiness monitor are legally attested in their respective roles	$\exists\ A_1, A_2, A_3, A_4, A_5 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_4) = uri$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_5) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) = uri)$

Table 8.26: IR3 linked and unique identity discretionary rules

$\beta_{IR3\text{-}D33\text{-}AP}$	The identity of the selected participant must be attested to by at least one evidence service provider • whose role has been attested to by a trustworthiness monitor • who confirms that the identifying attributes exist in corroborative evidence and the binding between an applicant and an identity was checked using one factor prior enrolment (ISO/IEC TS 29003:2018 Level 2), and there must be legal attestation for the evidence service provider and trustworthiness monitor in their respective roles.	$\exists\ A_1, A_2, A_3, A_4, A_5, A_6 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_4) =$ $ISO\text{-}IEC\text{-}29003{:}2018{:}Level2$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_5) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) = uri$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_6) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_6) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_6) = uri)$

Table 8.27: IR3 linked and unique identity discretionary rules

$\beta_{IR3\text{-}D34\text{-}AP}$	The identity of the selected participant must be attested to by at least one evidence service provider • whose role has been attested to by a trustworthiness monitor • who confirms that the identifying attributes exist in corroborative evidence and the binding between an applicant and an identity was checked using one factor prior enrolment (ISO/IEC TS 29003:2018 Level 3), and there must be legal attestation for the evidence service provider and trustworthiness monitor in their respective roles.	$\exists\ A_1, A_2, A_3, A_4, A_5, A_6 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = eIdentifier$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_4) =$ $ISO\text{-}IEC\text{-}29003{:}2018{:}Level3$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_5) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) = uri$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_6) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_6) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_6) = uri)$

Table 8.28: IR3 linked and unique identity discretionary rules

$\beta_{IR4\text{-}D021\text{-}AP}$	For each role that the selected participant has attestations for, there must be at least one role attestation that is not self-attested	$\exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = \mathcal{A}ttestation_{t_{val}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) \neq \mathcal{A}ttestation_{a_{id}}(A_1))$

Table 8.29: IR4 Discretionary rules/others

$\beta_{IR4\text{-}D022\text{-}AP}$	If the selected participant acts in the role of an accreditation body then this role must be attested to by a member of the International Attestation Forum (IAF) as conforming to ISO/IEC 17011 [174]	$\exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{AB}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = ISO\text{-}IEC\text{-}17011\text{:}2017$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) \in \{IAF\text{-}Memberlist\})$

Table 8.30: IR4 Discretionary rules/AB

$\beta_{IR4\text{-}D023\text{-}AP}$	If the selected participant acts in the role of a conformity assessment body then this role must be attested to by a member of the European Accreditation co-operation mechanism (EA) as conforming to ISO/IEC 17065 [176]	$\exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{CAB}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = ISO\text{-}IEC\text{-}17065\text{:}2012$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) \in \{EA\text{-}Memberlist\})$
$\beta_{IR4\text{-}D024\text{-}AP}$	If the selected participant acts in the role of a conformity assessment body then this role must be attested to by a member of the European Accreditation co-operation mechanism (EA) as conforming to ETSI EN 319 403 [88]	$\exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{CAB}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = EN319403$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) \in \{EA\text{-}Memberlist\})$

Table 8.31: IR4 Discretionary rules/others/CAB

$\beta_{IR4\text{-}D025\text{-}AP}$	If the selected participant acts in the role of an evidence service provider then this role must be attested to by a member of the European Accreditation co-operation mechanism (EA) as conforming to ISO/IEC 27001 [177]	$\exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = ISO\text{-}IEC\text{-}27001{:}2013$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2) \in \{EA\text{-}Memberlist\})$
$\beta_{IR4\text{-}D026\text{-}AP}$	If the selected participant acts in the role of an evidence service provider then this role must be attested to by a trustworthiness monitor	$\exists\ A_1 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EvSP}$ $\rightarrow \exists\ A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{a_{id}}(A_1) = \mathcal{A}ttestation_{t_{sub}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{TwsMo}))$
$\beta_{IR4\text{-}D027A\text{-}AP}$	If the selected participant acts in the role of an evidence service provider then this role must be attested to as conforming to the requirements of an eIDAS TSP by inclusion in a European Trusted List by a trustworthiness monitor	$\exists\ A_1, A_2, A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = isRegisteredIn$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = eIDASTrustList$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo})$
$\beta_{IR4\text{-}D027B\text{-}AP}$	If the selected participant acts in the role of an evidence service provider then this role must be attested to as conforming to the requirements of an eIDAS TSP by demonstrating conformance to ETSI EN 319 403 [87]	$\exists\ A_1, A_2, A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = ETSI\text{-}EN\text{-}319\text{-}403$

Table 8.32: IR4 Discretionary rules/others/EvSP

$\beta_{IR4\text{-}D028\text{-}AP}$	If the selected participant acts in the role of claim status service provider then this role must be attested to by a member of the European Accreditation co-operation mechanism (EA) as conforming to ISO/IEC 27001 [177]	$\exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{CsSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = ISO\text{-}IEC\text{-}27001\text{:}2013$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_2)\ in\ \{EA\text{-}Memberlist\})$
$\beta_{IR4\text{-}D029\text{-}AP}$	If the selected participant acts in the role of a claim status service provider then this role must be attested to by a trustworthiness monitor	$\exists\ A_1 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{CsSP}$ $\rightarrow \exists\ A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{a_{id}}(A_1) = \mathcal{A}ttestation_{t_{sub}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{TwsMo}))$
$\beta_{IR4\text{-}D030\text{-}AP}$	If the selected participant acts in the role of claim status service provider then this role must be attested to as conforming to the requirements of an eIDAS TSP by inclusion in a European Trusted List by a trustworthiness monitor	$\exists\ A_1, A_2, A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_l)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{CsSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = isRegisteredIn$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = eIDASTrustList$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = R_{TwsMo})$

Table 8.33: IR4 Discretionary rules/others/CsSP

$\beta_{IR4\text{-}D301\text{-}AP}$	Participants in the role of endorser that endorse the rulebook selected by the trustor must be attested by a legal act	$\forall\ P_{Endo} \in S_{PT}\ \exists\ A_1, A_2, A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_{Endo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnDo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_{Endo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesEndorse)$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = f_{id}(RBK_{id})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = f_{id}(P_{Endo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = uri)$
$\beta_{IR4\text{-}D302\text{-}AP}$	Participants in the role of enforcer that enforce the rulebook selected by the trustor must be attested by a legal act	$\forall\ P_{Enfo} \in S_{PT}\ \exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_{Enfo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnFo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_{Enfo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesEnforce)$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = f_{id}(RBK_{id})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = f_{id}(P_{Enfo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = uri)$

Table 8.34: IR4 Discretionary rules/legal qualifications

$\beta_{IR4\text{-}D303\text{-}AP}$	If the selected participant is an evidence service provider or claim status provider, it must be conformity assessed by a CAB that is accredited by a legally qualified AB	$\exists\ P_1, P_{AB}, P_{CAB} \in S_{PT}\ \exists\ A_1, A_2, A_3, A_4, A_5 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = (R_{EvSP} \vee R_{CsSP})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_{AB})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{AB}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = f_{id}(P_{AB})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = uri$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = f_{id}(P_{AB})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = doesAccredit$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_4) = f_{id}(P_{CAB})$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_5) = f_{id}(P_{CAB})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_5) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_5) = doesConformTo$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_5) = STANDARD^{11}$))
$\beta_{IR4\text{-}D304\text{-}AP}$	If the selected participant is an evidence service provider or claim status provider, it must be monitored by a trustworthiness monitor attested by a legal act	$\exists\ P_1, P_{TwsMo} \in S_{PT}\ \exists\ A_1, A_2, A_3, A_4 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = (R_{EvSP} \vee R_{CsSP})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_3) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = doesSupervise$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_4) = uri)$

Table 8.35: IR4 Discretionary rules/legal qualifications

$\beta_{IR4\text{-}D305\text{-}AP}$	If the selected participant is an evidence service provider or claim status provider, it must be monitored by a trustworthiness monitor registered in a European trusted list	$\exists\ P_1, P_{TwsMo} \in S_{PT}\ \exists\ A_1, A_2, A_3, A_4 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = (R_{EvSP} \vee R_{CsSP})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_3) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = doesSupervise$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = eIDAS\_Supervisory\_Body$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_4) = uri)$

Table 8.36: IR4 Discretionary rules/legal qualifications

$\beta_{IR5\text{-}D0A\text{-}AP}$	The potential trustee is an actor that agrees to the rulebook specified in the invocation of the trustworthiness evaluation function	$(\text{Actor}(P_I)$ $\wedge\ (\exists\ A \in S_{agr}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A) = doesAgree$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A) = RBK_{id}))$
$\beta_{IR5\text{-}D0B\text{-}AP}$	The rulebook specified in the invocation of the trustworthiness evaluation function must be endorsed by at least one endorser	$\exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnDo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesEndorse)$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = RBK_{id})$
$\beta_{IR5\text{-}D0C\text{-}AP}$	The rulebook specified in the invocation of the trustworthiness evaluation function must be enforced by at least one enforcer	$\exists\ A_1, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnFo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_I)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesEnforce)$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = RBK_{id})$

Table 8.37: IR5 Discretionary rules/agreement, endorsement, enforcement

$\beta_{IR5\text{-}D01\text{-}AP}$	For the rulebook chosen by the trustor, there exists an endorser who discloses information of who takes on responsibility, accountability, and authority to implement information security governance in a self-attested attestation	$\exists\ P_{Endo} \in S_{PT}\ \exists\ A_1, A_2, A_3 \in S_{attn}\ \exists\ RBK_{id} \in S_\beta$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_{Endo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnDo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_{Endo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesEndorse)$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = f_{id}(RBK_{id})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_1) = \mathcal{A}ttestation_{t_{sub}}(A_3)$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_3) = \mathcal{A}ttestation_{t_{sub}}(A_3)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = doesDisclose$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = uri)$
$\beta_{IR5\text{-}D02\text{-}AP}$	For the rulebook chosen by the trustor, there exists a legally qualified endorser who discloses information of who takes on responsibility, accountability, and authority to implement information security governance in a self-attested attestation	$\exists\ P_{Endo} \in S_{PT}\ \exists\ A_1, A_2, A_3, A_4 \in S_{attn}\ \exists\ RBK_{id}$ $\in S_\beta$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_{Endo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnDo}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_{Endo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = doesEndorse)$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = f_{id}(RBK_{id})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_1) = \mathcal{A}ttestation_{t_{sub}}(A_3)$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_3) = \mathcal{A}ttestation_{t_{sub}}(A_3)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = doesDisclose$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_3) = uri$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_4) = f_{id}(PT)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_4) = uri)$

Table 8.38: IR5 Discretionary rules/disclosure

$\beta_{IR5\text{-}D11\text{-}AP}$	If the selected participant is an endorser, it cannot be an enforcer	$\forall\, A_1 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_1)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnDo}$ $\rightarrow \nexists\, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_1)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EnFo}))$
$\beta_{IR5\text{-}D12\text{-}AP}$	If the selected participant is an enforcer it cannot be an endorser	$\forall\, A_1 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_1)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_1) = R_{EnFo}$ $\rightarrow \nexists\, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_1)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_2) = R_{EnDo}))$

Table 8.39: IR5 discretionary rules regarding mutual exclusion of endorser and enforcer

$\beta_{IR5\text{-}D21\text{-}AP}$	Helper rule that defines the separation of duties in the enabler plane	$S_{SOD_1} = \{R_{EnDo}, R_{EnFo}, R_{AB}, R_{CAB}\}$
$\beta_{IR5\text{-}D22\text{-}AP}$	If the selected participant is in S_{SOD_1} then only one role is allowed	$\forall\, A_1 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_1)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_1) \in S_{SOD_1}$ $\rightarrow \neg\, \exists\, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_1)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_2) \in S_{SOD_1}))$

Table 8.40: IR5 discretionary rules regarding separation of duty for the enabler plane

$\beta_{IR5\text{-}D23\text{-}AP}$	Separation of duties for the trustworthiness monitor role	$\forall\, A_1 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(P_1)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\, \mathcal{A}ttestation_{t_{val}}(A_1) = R_{TwsMo}$ $\rightarrow \nexists\, A_2 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}(A_2) = f_{id}(P_1)$ $\wedge\, \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\, (\mathcal{A}ttestation_{t_{val}}(A_2) = R_{EvSP}$ $\vee\, \mathcal{A}ttestation_{t_{val}}(A_2) = R_{CsSP})))$

Table 8.41: IR5 discretionary rule regarding separation of duty for the trustworthiness monitor role

Chapter 9

Evaluating trustworthiness

This chapter presents an approach to evaluating trustworthiness. It builds on the preceding chapters in which data and constraints over the data have been defined. A working definition of trustworthiness was proposed in Section 5.2.2, and an approach to evaluating trustworthiness was proposed in Section 6.7. This approach is now specified in detail.

9.1 Introduction

This chapter is concerned with the functions used to evaluate trustworthiness. Three possible such functions were introduced in Section 6.7, namely $twseval_{AE}$ (for evaluating the trustworthiness of an entire ecosystem), $twseval_{AP}$ (for evaluating the trustworthiness of a participant), $twseval_{P}$ (for evaluating the trustworthiness of a transaction). Only the first two are described in detail here – the third remains a possible topic for future research. This chapter provides detailed specifications of the functions $twseval_{AE}$ and $twseval_{AP}$, including details of their input parameters and how they can be used.

Section Section 9.2 provides details of the ecosystem evaluation function $twseval_{AE}$, and Section 9.3 addresses the participant evaluation function $twseval_{AP}$. A brief summary is provided in Section 9.4.

9.2 The ecosystem evaluation function $twseval_{AE}$

This function is invoked by a trustor to assist in deciding to what extent an ecosystem represented by instance data can be regarded as trustworthy. The remainder of this section describes the function parameters and lists the tables from which discretionary rules can be selected.

9.2.1 Function signature

The function signature is

$$twseval_{AE}(R_{id}, \{DiscretionaryRules\}, InstanceData)$$

where

- R_{id} identifies the applicable rulebook,
- $\{DiscretionaryRules\}$ denotes the set of discretionary rules selected by the trustor, and
- *InstanceData* identifies the instance data that is to be used.

Execution of the function includes verification of the mandatory rules of the selected rulebook.

The function returns *true* when all of the evaluated rules return *true*. *True* means that the evaluated ecosystem meets the constraints specified in the rules, which is an indication of trustworthiness.

The function returns *false* when at least one of the evaluated rules returns *false*. *False* means that the evaluated ecosystem does not meet the constraints specified in the rules, which is an indication of a lack of trustworthiness.

9.2.2 Selection of discretionary constraints

9.2.2.1 IR2 Transparency

Rules can be selected to express a policy regarding transparency from the following tables.

- Enabler plane rules can be selected from Table 8.1.
- Trustworthiness provision plane rules can be selected from Table 8.2.
- Functional plane rules can be selected from Table 8.3.

9.2.2.2 IR3 Linked and unique identity

Rules can be selected to express a policy regarding participant identity from the following tables.

- A single rule regarding self-attestation can be selected from Table 8.5,
- Rules regarding other-attestations can be selected from Tables 8.6 and 8.7.
- Rules regarding attestion by legally qualified others can be selected from Tables 8.8, 8.9 and 8.10.

9.2.2.3 IR4 Competently acting in role

Rules can be selected to express a policy regarding participant competence from the following tables.

- The single rule regarding having at least one role attestation that is not self-attested can be selected from Table 8.12.
- The single rule regarding accreditation bodies can be selected from Table 8.13.
- Rules regarding conformity assessment bodies can be selected from Table 8.14.
- Rules regarding evidence service providers can be selected from Table 8.15.
- Rules regarding claim status service provider can be selected from Table 8.16.
- Rules regarding attestations by legally qualified others can be selected from Tables 8.17 and 8.18.

9.2.2.4 IR5 Governance, security and controls

Rules can be selected to express a policy regarding participant governance, security and controls from the following tables.

- Rules regarding compliance with IT governance can be selected from Table 8.19.
- Rules regarding separation of duty can be selected from Table 8.20, Table 8.21 and Table 8.22.

9.3 The participant evaluation function $twseval_{AP}$

This function is invoked by a trustor to assist in deciding to what extent a participant P_1 can be regarded as trustworthy in a particular role. We next describe the following elements:

- the signature of the $twseval_{AP}$ function;
- the tables from which discretionary rules can be selected without modification;
- possible refinements of discretionary rules where this is enabled by using the information specified in the function invocation; including the potential trustee, the rulebook to be used and standards to be complied with.

9.3.1 Function signature

The function signature is

$twseval_{AP}(RBK_{id}, P_1, target\_base\_role\_P_1, \{DiscretionaryRules\}, InstanceData, \{Norms\})$

where

- RBK_{id} identifies the applicable rulebook,
- P_1 identifies the potential trustee,
- $target\_base\_role\_P_1$ denotes the target base role of P_1, i.e. the role in which the trustee is being evaluated,
- $\{DiscretionaryRules\}$ stand for the set of discretionary rules selected by the trustor,
- *InstanceData* refers to the instance data that is to be used, and
- $\{Norms\}$ denotes the set of discretionary norms against which the trustee is to be conformity assessed.

Execution of the function includes verification of the mandatory rules of the selected rulebook.

The function returns *true* when all of the evaluated rules return *true*. *True* means that the evaluated participant meets the constraints specified in the rules, which is an indication of trustworthiness.

The function returns *false* when at least one of the evaluated rules returns *false*. *False* means that the evaluated participant does not meet the constraints specified in the rules, which is an indication of a lack of trustworthiness.

9.3.2 Selection of discretionary constraints

9.3.2.1 IR2 Transparency

For IR2 Transparency, there are no discretionary rules, because transparency is already addressed for the purpose of $twseval_{AP}$ by the mandatory rules.

9.3.2.2 IR3 Linked and unique identity

These rules can be selected from Tables 8.23 – 8.28.

9.3.2.3 IR4 Competently acting in role

These rules allow selection of a policy determining how participant competence is evaluated. They can be selected from Tables 8.29 – 8.33.

9.3.2.4 IR5 Governance, security and controls

These rules allow selection of a policy determining the basis for evaluating participant governance, security and controls. The rules regarding agreement, endorsement and enforcement can be selected from Table 8.37. The two rules regarding legal qualification of endorser and enforcer can be selected from Table 8.38. Regarding separation of duty, the rules can be selected from Tables 8.39 – Table 8.41.

9.4 Summary

Two trustworthiness evaluation functions were specified: $twseval_{AE}$, to be used for evaluating the trustworthiness of an entire ecosystem, and $twseval_{AP}$ to be used for evaluating the trustworthiness of a participant. In both cases the function signature was defined, and the use of the function was described.

Part III

Using trust and trustworthiness

Chapter 10

Overview and implementation choices

To demonstrate the practical feasibility of the $\mathcal{TE}$ framework, a partial implementation is presented in this and the next five chapters. Possible implementation choices for the data model, rulebook, trustworthiness evaluation functions and instance data are compared and chosen on the basis of defined selection criteria. The implementation is then described.

10.1 Introduction

This chapter introduces the third part of the thesis, in which partial implementations of the data model, rulebook and trustworthiness evaluation functions are presented. To help ensure its practical relevance, the selection and storage of instance data is also addressed. The implementation was performed in two phases.

- In the first phase, selection criteria were formulated and used to determine the appropriate technical components. An implementation architecture was defined to help ensure effective interaction between the components. The first phase forms the focus of this chapter.
- In the second phase, the data model, a specific rulebook, trustworthiness evaluation functions and instance data were implemented and tested. These are described in Chapters 11 – 14.

Conclusions and ideas for future work are given in Chapter 16.

This chapter describes the first phase of the implementation. Possible approaches to implementation are introduced and compared in Section 10.2. The data model, rulebook, trustworthiness evaluation functions and instance data are addressed. Implementation choices were

selected on the basis of defined selection criteria. Section 10.3 describes the architecture and the technical components that were selected for implementation. Section 10.4 provides a summary.

10.2 Evaluation of implementation choices

10.2.1 Data model

10.2.1.1 Selection criteria

The following criteria were used for the selection of the technology for the data model implementation.

- Well-defined syntax and semantics must be supported. This is required for transparency and general understanding.
- A truth-functional interpretation must be supported. This is required because, as described in Section 7.2, the data for the $\mathcal{TE}$ framework is specified as predicates which have a truth-functional interpretation.

10.2.1.2 Alternatives

Possible ways of modelling data include the following.

- In a *relational model*, information is modelled in tables consisting of rows and columns. The tables are related by primary keys and foreign keys. A primary key is a specific choice of a minimal set of columns that uniquely specify a row in a table. A foreign key is a set of columns in a table that refers to the primary key of another table, linking these two tables. Relational databases are a widely used implementation of such a data model, with SQL[1] as the most popular query language.
- In a *key-value model*, information is represented as a collection of key–value pairs, stored in an associative array. Such an array is an abstract data type composed of a collection of key-value pairs such that each possible key appears at most once in the collection. This model is used to model data that can be represented in such pairs, which includes wide column data and entire documents. The many existing NoSQL database systems[2] provide implementations of such a model.
- *Hierarchical trees*, as used by the eXtensible Mark-up Language (XML) model, are another way of representing information. Implementations can be found in the NoSQL

[1] See e.g. `https://en.wikipedia.org/wiki/SQL`
[2] See e.g. `https://en.wikipedia.org/wiki/NoSQL`

database family, particularly in the document-related subfamily including databases oriented towards XML and other document formats.

- *Semantic models* such as RDF, RDF Schema and OWL represent data as a graph. Triplestores and graph databases offer common implementations, and are available from many suppliers including TopQuadrant[3], Ontotext[4], the Apache Software Foundation[5] and OpenLink Software[6].

All four alternatives are based on a well-defined syntax. However, they differ in their support for semantics.

- The first three alternatives represent syntactical structures. Data typing can be used to add meaning. Truth-functional interpretation is not present in these models; instead it must be created on top of the syntax. Therefore they do not offer a suitable alternative for the implementation of the data model for the trustworthiness evaluation system.
- The fourth alternative consists of a class of modelling alternatives specifically designed to support semantic modelling. Within this class, OWL has good support for semantics. RDF models data as a graph consisting of sets of (subject, predicate, object)-triples, with semantics defined accordingly. New triples can be added to the graph, and may be linked to any existing subject, predicate or object. OWL extends RDF's possibilities to capture semantics. A discussion of RDF and OWL is provided in Section 4.3.

10.2.1.3 Selection

On the basis of the assessment in the preceding section, a combination of RDF and OWL was selected for data modelling because this best meets the defined requirements.

10.2.2 Implementation of rulebooks and evaluation

The representation of rulebooks and the evaluation of the rules they contain are both based on logic, and are also tightly coupled. They are therefore treated together.

10.2.2.1 Selection criteria

The following selection criteria were used for the selection of components to implement rulebooks and their evaluation.

[3] `https://www.topquadrant.com/`
[4] `https://www.ontotext.com/`
[5] `https://apache.org/`
[6] `https://www.openlinksw.com/`

- As for the data model, well-defined syntax and semantics must be supported. This is required for transparency and general understanding. The syntax and meaning of the rules, and the outcome of their evaluation, must be available to everyone that uses them.
- The implementation must be based on a logic that is decidable[7], because otherwise there is no way to ascertain the correctness of the answer. Furthermore, the time required to derive the answer must be acceptable for users. The precise timeliness requirement depends on the use case. For example:
  - in on-line electronic commerce, users may need an answer in less than a second (or even less);
  - in a non-commercial context, users may be willing to accept longer periods of time.

  For the partial implementation that was created for the thesis it was assumed that the answer must be available in less than fifteen minutes.
- For practical reasons, the implementation of the logic must offer good integration with that of the data model.
- The implementation must use existing vocabularies or ontologies from well-known sources. This decreases the learning curve of users, and increases the chances of acceptance of the framework.

10.2.2.2 Alternatives

Possible choices for the language used to implement the logic include the following:

- a general purpose computer language such as Java,
- a domain specific language such as Erlang, HTML or Unix Shell Script,
- a language oriented towards logic processing, such as Prolog,
- the combination of a semantic language such as the Web Ontology Language (OWL), with a reasoning engine and a matching query language.

[7] In logic, a true/false decision problem is decidable if there exists an effective method for deriving the correct answer. Logical systems such as propositional logic are decidable if membership in their set of logically valid formulas (or theorems) can be effectively determined. A theory (set of sentences closed under logical consequence) in a fixed logical system is decidable if there is an effective method for determining whether arbitrary formulas are included in the theory. For a discussion see Section 2.3.1 or Mendelson [240].

General purpose languages are inherently transparent. However to implement the logic of the $\mathcal{TE}$ framework would require significant additional programming to integrate with data in the OWL semantics, and to guarantee decidability of the logic. The use of existing vocabularies would be complicated if not impossible. For example, Java's object-oriented data model does not offer much support for integration with semantic models, and neither does Java include a rule engine. Should one want to use such a language for the implementation of the $\mathcal{TE}$ framework, then most functionality would have to be created from scratch. As a result, the use of a general-purpose language was not pursued.

Domain-specific languages are created specifically to solve problems in a particular domain. They are not intended to be able to solve problems outside of this domain, although that may be technically possible. The survey given in Chapter 3 does not identify a domain-specific language suitable for implementing the logic of the $\mathcal{TE}$ framework. We therefore did not pursue this option further.

Languages such as Prolog combine transparency with a sound logic foundation. Prolog is an untyped declarative language where the program logic is expressed in terms of relations, represented as facts and rules. A computation is initiated by running a query over these relations. Prolog is based on FOL Horn clauses and is Turing complete[8]. Prolog uses a non-deterministic evaluation strategy to solve a query, so decidability is not guaranteed. For this reason the cut operator[9] and other language constructs have been introduced into the language. The cut operator makes Prolog not purely declarative and a procedural reading of a program is needed to understand it. Prolog has also been used for applications in the semantic web, as described by Wielemaker et al. [384]. However, the following issues arise with such a choice.

- Only a limited number of implementations that combine Prolog or Datalog with semantic web data could be identified.
- A short preliminary analysis suggested that such a combination is rather complex.
- Implementing rules on the basis of existing vocabularies and ontologies is not straightforward.

[8] A system of data-manipulation rules (such as a computer's instruction set or a programming language) is said to be Turing-complete if it can be used to simulate any Turing machine (a mathematical model of computation built on an abstract machine that manipulates symbols on a strip of tape according to a table of rules). This means that this system is able to recognize or decide other data-manipulation rule sets. Turing completeness is used to express the power of such a data-manipulation rule set. A system that is Turing-complete is also referred to as computationally universal. Most computer languages today are Turing-complete. Datalog is a subset of Prolog which is not Turing-complete. For a detailed treatment of Turing-completeness see, for example, the article on Turing in the Stanford Encyclopedia of Philosophy [149]

[9] The cut operator is a goal, written as !, which always succeeds, but cannot be backtracked. It is used to prevent unwanted backtracking, including finding extra solutions and avoiding unnecessary computations

In conclusion, while in principle such a language could be used, there appear to be considerable practical difficulties with such an approach.

The combination of a semantic web language such as the Web Ontology Language (OWL) with a reasoning engine and a matching query language (SPARQL) has the following advantages.

- It provides the required degree of transparency, because OWL allows annotations to the data model which can be used to explain the deductions made by the reasoning engine.
- The use of a reasoner, which is typically built-in in an OWL environment, allows the maintenance of consistency and simplicity in data models and in the formulation of queries.
- A type of OWL can be selected that is a decidable fragment of FOL.
- Existing vocabularies and ontologies can be imported and used as a basis to construct new elements.

10.2.2.3 Selection

On the basis of the assessment in the preceding section, the combination of the logic supported by RDF and OWL with a reasoning engine and a query language was selected to implement the logic required for the $\mathcal{TE}$ framework.

10.2.3 Instance data

10.2.3.1 Selection criteria

The selection criteria for instance data are based on requirement IR7, introduced in Section 5.5.7:

As a participant in an electronic ecosystem I can understand the origin and the type of data that is used in the evaluation of trustworthiness of participants, so that I can claim the outcome of the trustworthiness evaluation is based on credible data.

For the trustworthiness evaluation to be based on credible data, such data must come from authoritative sources that allow access to data that corresponds to one or more predicates. This leads to the following selection criteria.

- The data source must offer relevant data, i.e. data specified in the data model. This means that the data must be mappable to one or more predicates specified in the $\mathcal{TE}$ data model.
- The data source must be authoritative for this data.

- The data must include a description of its meaning.
- The data must be available in a machine-readable format. If the data is also available in a human readable format, this is additionally valuable.

10.2.3.2 Alternatives

There are many data sources capable of providing data corresponding to one or more predicates. The implementation described below limits itself to data sources in the public domain. An analysis of available data sources is described in Chapter 12.

10.2.3.3 Selection

The selection of data sources and instance data for each data element of the $\mathcal{TE}$ data model is addressed in Chapter 12.

10.3 Implementation architecture and tooling

10.3.1 Architecture

Combining the elements selected above leads to the architecture depicted in Figure 10.1.

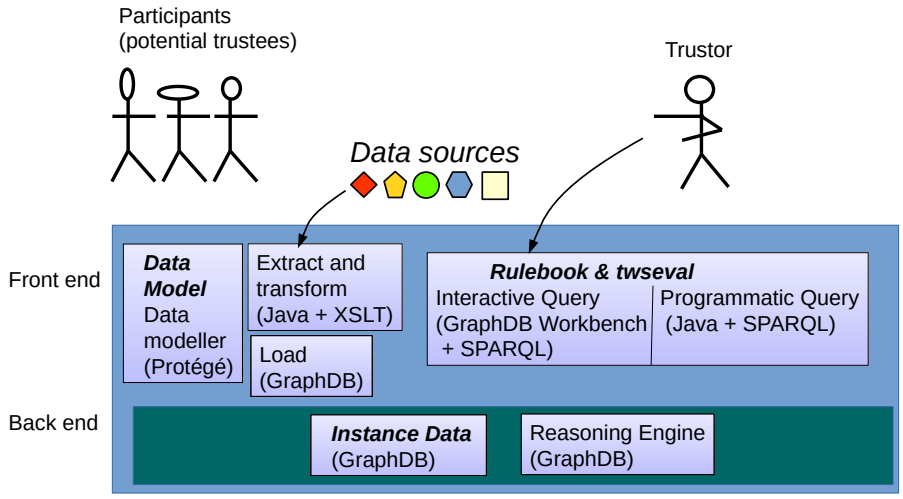

Figure 10.1: Implementation architecture.

The following elements are included.

- A set of participants as potential trustees, and a potential trustor.

- Data sources in the public domain, as discussed in Chapter 12.
- A front end layer, composed of the following elements.
  - The $\mathcal{TE}$ data model, created using Protégé [250], see Section 10.3.2.
  - Extract and transform programs which download information from the data sources and transform it into the form required by the implementation of the $\mathcal{TE}$ data model. These are written in a combination of the general purpose language Java and Extensible Stylesheet Language Transformations [377] (XSLTs). XSLT is a language for transforming XML documents into other XML documents. To load the transformed information into the back end, the standard load utility of the Graph DB database was used.
  - An implementation of the rulebook and trustworthiness evaluation functions.
    * The interactive query interface is based on GraphDB's Workbench, which is an interactive interface to the GraphDB database[10]. The rulebook is implemented as a set of SPARQL queries that are stored and executed in the Workbench.
    * The programmatic query interface consists of an Eclipse development environment, in which SPARQL and Java are combined to form the rulebook and the evaluation functions. The Java code is used to drive the execution of the SPARQL queries and does not implement the evaluation logic.
- A back end layer, composed of:
  - the instance data, stored in an Ontotext GraphDB database;
  - the internal reasoning engine included in the database.

10.3.2 Data model

Protégé [250] was used as the data modelling tool. It is a free, open-source ontology editor, developed by the Stanford Center for Biomedic Medicine[11]. It supports the OWL 2 Web Ontology Language and RDF specifications from the World Wide Web Consortium.

It includes a built-in HermiT reasoner [127], which was used for consistency checking of the model. The built-in OntoGraf[12] feature was used to visualise the ontology.

In initial implementation development work, Protégé also served as the SPARQL engine. However, its SPARQL queries do not take into account inferred data and are hence limited. Therefore the model and its data were moved into a back-end database whose SPARQL engine does support queries on inferred data. The set-up of Protégé is further detailed in Section 11.3.

[10] `https://graphdb.ontotext.com/`
[11] `https://protege.stanford.edu/about.php\#about-bmir`
[12] `https://protegewiki.stanford.edu/wiki/OntoGraf`

10.3.3 Data import and transformation

To load the selected instance data into the GraphDB database, XSL transformations were developed using an Eclipse development environment[13]. The Xalan Java libraries[14] were used for XSLT and XPath processing. The transformations were tailor-made to transform a specific input (data source) to a specific output (a predicate in the form of an OWL assertion).

10.3.4 Database

10.3.4.1 GraphDB functionality

The free edition of Ontotext's GraphDB[15] version 8.8 was used as the back-end database. GraphDB includes its own TRREE[16] reasoner for consistency checking. It also includes a SPARQL 1.1 query engine.

GraphDB supports four of the OWL species[17] introduced in Section 4.3.6.1. Their semantics and inference are defined in GraphDB internal rule-sets. Details can be found in the GraphDB documentation[18]. Of these four species, the OWL Max ruleset was used. It covers the full RDFS semantics without limitations, apart from the entailment related to typed literals (known as D-entailment), most of OWL Lite and all of OWL DLP.

Regarding the type of inference, the *OWL Max* rule-set was selected because it covers the semantics and inference required for the implementation of the $\mathcal{TE}$ framework. The detailed set-up of the database is specified in Section 12.3.2.

10.3.5 Rulebook and trustworthiness evaluation

10.3.5.1 Interactive query

The interactive query front end consists of the GraphDB Workbench, a graphical user interface to the GraphDB database. The rulebook is implemented as a set of SPARQL queries. These are stored and can be executed in the GraphDB Workbench, along with the instance data. The set-up is described in Section 13.3.2.

[13]The version 'Eclipse IDE for Java Developers Version: Mars.1 Release (4.5.1)' was used
[14]`https://xalan.apache.org/`
[15]`https://graphdb.ontotext.com/`
[16]Triple Reasoning and Rule Entailment Engine
[17]OWL Horst, OWL Max, OWL2 QL, and OWL2 RL.
[18]GraphDB Free Documentation Release 8.7 Ontotext, Oct 22, 2018

10.3.5.2 Programmatic query

Programmatic queries were developed using an Eclipse[19] development environment. The rulebook and trustworthiness evaluation functions that were written for use in the interactive queries were embedded in Java programs. These programs use a database driver to connect to the GraphDB where the instance data resides. This set-up was used for prototyping but not for the implementation.

10.4 Summary

This chapter described the first phase of the implementation. Possible approaches to the implementation of the data model, rulebooks, trustworthiness evaluation functions and instance data were introduced and compared. Selection criteria were specified and the choices for implementation were made on this basis. The main choices were the use of a decidable version of OWL for data modelling, the reuse of existing ontologies to improve interoperability, and the integration with the real world through the selection of public data sources. The implementation architecture and the selected technical components were presented. The main components are:

- Protégé, as the OWL data modelling tool,
- Java and XSLT, to extract data from the selected sources and transform it into the data model,
- GraphDB, to store the transformed information and make it available to the evaluation functions.

[19] `https://www.eclipse.org/`

Chapter 11

Implementation of the data model

This chapter presents an implementation of the data model that was specified in Chapter 7.

11.1 Introduction

This chapter describes the OWL DL implementation of the data model specified in Chapter 7. The choice of OWL DL was discussed in 10.2.1. A fundamental part of the implementation was the choice of OWL classes and properties to implement the predicates of the model. The question of whether to create an ontology from scratch or to incorporate one or more existing ontologies is addressed. After the identification of candidate ontologies, we describe how the selected approach was chosen. Where possible, classes and properties from the incorporated ontologies were reused.

The processes used to load the model implementation into a database and to import instance data are described in Chapter 12. The implementations of a specific rulebook and of trustworthiness evaluation functions are described in Chapters 13 and 14.

Section 11.2 describes the approach that was followed. Section 11.3 explains the set-up of Protégé, the tool that was used for data modelling. Two further sections cover subjects that are relevant to more than a single predicate:

- Section 11.4 specifies how time and commitments are modelled;
- Section 11.5 specifies how unique identity is modelled.

The approaches used to model the predicates of the data model as OWL classes and properties are described in Sections 11.6 – 11.11.

- Section 11.6 describes the implementation of the specific rulebook used in the thesis.

- Section 11.7 specifies how participants are modelled.
- Section 11.8 specifies how agreements are modelled.
- Sections 11.9 and 11.10 specify how endorsement and enforcements are modelled.
- Section 11.11 specifies how attestations are modelled.

Section 11.12 describes how data sources are modelled, and afterwards Section 11.13 provides an overview of the classes and properties that were used. Section 11.14 provides a summary of the chapter.

11.2 Approach

11.2.1 To create from scratch or reuse?

To create the $\mathcal{TE}$ data model, a dedicated $\mathcal{TE}$ OWL ontology `http://www.marcsel.eu/onto/te/` was specified. The terminology defined in Hitzler et al. [148] was used. An introduction to OWL is provided in Section 4.3.6 and its use for data modelling is described in appendix D.

When creating an ontology it is necessary to decide whether to start from scratch and define all the necessary concepts, or to include one or more already existing ontologies and reuse the defined meanings. The two approaches have the following advantages and disadvantages.

- Creating an ontology from scratch.
  - This has the advantage of giving its creator complete freedom over all aspects of the ontology.
  - It has the disadvantage of not capitalising on definitions of meaning that have been vetted and documented, and in some cases well-accepted and in use.
- Reusing one or more existing ontologies.
  - This has the advantage of capitalising on existing definitions of meaning, which brings the following benefits.
    * It has the potential to reduce errors, since ontologies that have been published by organisations such as the Worldwide Web Consortium have been created through a controlled process and are less likely to contain serious errors.
    * It improves interoperability with existing Semantic Web applications based on existing ontologies.

    - It decreases the amount of new terminology users have to learn. This improves the chances of the new ontology being accepted in a wider user community.
  - It has the disadvantage of leaving less freedom to its creator.

Given the above-listed advantages of ontology re-use, the decision was made to re-use existing ontologies in implementing the $\mathcal{TE}$ data model.

11.2.2 Existing ontologies

Given the decision to re-use existing ontologies, it was necessary to first understand available alternatives. The following sources of information on ontologies were used:

- the DARPA Agent Markup Language (DAML) list of ontologies[1],
- the W3C's list of ontologies[2],
- the Protégé list of ontologies[3],
- the Object Management Group (OMG) ontologies[4], and
- the Global Legal Entity Identifier Foundation (GLEIF) ontologies[6].

Also, ISO/IEC is soon expected to publish two documents on ontologies:

- ISO/IEC PRF 21838-1 [183] Information technology — Top-level ontologies (TLO) — Part 1: Requirements, and
- ISO/IEC PRF 21838-2 [184] Information technology — Top-level ontologies (TLO) — Part 2: Basic Formal Ontology (BFO).

However at the time the implementation was developed these were not available, and were thus not considered.

11.2.3 Selected ontologies

Of the ontologies listed above, an analysis revealed that the following were relevant to the implementation of the data model.

[1] `http://www.daml.org/ontologies/`
[2] `https://www.w3.org/wiki/Lists_of_ontologies`
[3] `https://protegewiki.stanford.edu/wiki/Protege_Ontology_Library`
[4] `https://www.omg.org/hot-topics/finance.htm` and their implementation by the EDM Council (EDMC)[5]
[6] `https://www.gleif.org/ontology/`

- Two ontologies from the W3C:
  - the Organization[7] (ORG) ontology [376], which enables the publication of information on organisations and organisational structures;
  - the Provenance (PROV-O) ontology [357] which enables tracing the provenance of an object or entity, and provides contextual and circumstantial evidence for its original production.
- Two ontologies from the EDM Council, which enable the description of financial information:
  - the FIBO Foundations [77] ontology, and
  - the FIBO Business Entities [78] ontology.
- Two ontologies from the Global Legal Electronic Identifier Foundation (GLEIF), which enable the description of legal entities:
  - the GLEIF level 1 ontology [123] , and
  - the Entity Legal Form (ELF) ontology [122].

Background information to these ontologies, as well as how they were used, is provided in Appendix D.2.

11.3 Set-up

11.3.1 Protégé

Protégé, as described in 10.3.2, was used as the data modelling tool. The chosen syntax is RDF/XML. Details of naming conventions, character encoding and namespaces are discussed in Appendix D.1.2.

11.3.2 Mapping predicates onto OWL DL

A dedicated $\mathcal{TE}$ ontology was specified. The prefix *te* was defined as `http://www.marcsel.eu/onto/te/`. Predicates are modelled as OWL classes and properties of this ontology. For example the predicate Participant is implemented as the *te:Participant* class, and properties include *te:pAgreement* and *te:pEndorsement*. An actual Participant, represented by instance data, is implemented as an individual of the *te:Participant* class. Time and commitment marks are not implemented.

[7] The W3C uses the American spelling

11.3.3 Location

The ontology that represents the data model is available at `http://www.marcsel.eu/onto/te/te-data-model.owl`.

11.3.4 Importing existing ontologies

The TE ontology imports two existing ontologies:

- the ORG ontology, from `http://www.w3.org/ns/org\#`, and
- the PROV ontology, from `http://www.w3.org/ns/prov-o-20130430`.

Depending on the tool used, these might be loaded automatically or an import[8] action might be needed.

11.4 Time and commitment

11.4.1 Time

It must be possible to relate the notions of points in time, including start and end points of an interval, and of interval duration to individuals of the classes of the $\mathcal{TE}$ data model. For this purpose two classes are defined.

- The class *te:TimeInstant* represents points in time such as start and end points.
- The class *te:TimeInterval* represents intervals which have a start and end point. It has two subclasses.
  - *te:Event* represents time intervals during which something eventful takes place.
  - *te:TemporalRelation* represents relations that connect at least two entities and last for an interval of time.

11.4.2 Commitment

There are many ways of expressing the commitment of an entity to information. This includes hashes, commitment schemes, message authentication codes, and electronic signatures. As the thesis is limited to the semantic aspects of evaluating trustworthiness, it is assumed that such a scheme may be in place. However, how such an commitment is instantiated is outside the scope of this thesis.

[8] E.g. in Protégé one may have to select the 'Active ontology/Ontology imports' tab, and perform a 'direct import' before the ontology that is referred to in an OWL import statement is actually loaded into the workspace.

11.5 Establishing unique identity

According to requirement IR3, specified in Section 5.5.3, all individuals in the $\mathcal{TE}$ framework need to be uniquely identified. Otherwise it would not be possible to implement trustworthiness evaluation functions that effectively verify segregation of duty rules.

For this purpose the class *te:ID* and corresponding properties were created[9].

- The class *te:ID* is defined as equivalent to *te:uniqueText* with the existential qualifier ('some').
- The data property *te:uniqueText* is defined as a functional property (meaning it can only have a single value), without domain, and with *xsd:string* as range. Its value corresponds to the eIdentifier. Who issues eIdentifiers is outside the scope of this thesis.
- The object property *doesIdentify* identifies things. It is defined as functional because an identifier should only identify a single thing in the $\mathcal{TE}$ data model.
- The inverse object property *identifiedBy* is defined for convenience. It is not functional since a thing can be identified by many identifiers, e.g. a citizen temporarily having residence abroad.

Uniqueness is enforced for the functional properties by the consistency checks that are performed by the reasoner. These checks are automatically performed at the initial loading of data into the OWL environment (modeller or database), and at run time when an insert operation is performed. This guarantees that all participants are uniquely identified.

This uniqueness is enforced during inference and for inference purposes, under the OWA[10]. OWL does not force the actual presence of a functional property. Such presence must be checked via SPARQL or any other means. Individuals of the class *te:ID* have a name that starts with *ID-*.

11.6 Rulebook

The concept of a rulebook is introduced in Chapter 8. For implementation purposes, a distinction is made between two ways of using a rulebook.

[9] OWL 2 supports the *HasKey* axiom, which states that each named instance of a class is uniquely identified by a (data or object) property or a set of properties. Hence if two named instances of the class coincide on values for each of key properties, then these two individuals are the same. However, this is not stringent enough for the $\mathcal{TE}$ data model because the model relies on an eIdentifier whose uniqueness must be enforced.

[10] All individuals that are different must also be specified as different in OWL.

- For the purpose of data modelling, it is necessary to represent rulebooks because they are terms of predicates such as agreements, endorsements and enforcements. This is addressed in the current chapter.
- For the purpose of trustworthiness evaluation, it is necessary to implement the rulebook rules. This is addressed in Chapter 13.

11.6.1 The *te:RuleBook* class

The class *te:RuleBook* is specified as a subclass of *owl:Thing*. There may be multiple rulebook individuals. Each individual is uniquely identified using an identifier of the class *te:ID* and the object property *te:doesIdentify*.

Individuals of the *te:RuleBook* class allow participants to express their compliance with the specified rulebook through an agreement, and let endorsers and enforcers express their endorsement and enforcement thereof.

11.6.2 The rulebook digests

An individual of the class *te:RuleBook* is linked with its rules through the data properties *te:ruleBook-digest-RIPEMD-160* and *te:ruleBook-digest-SHA-256*. These data properties contain the RIPEMD-160 [168] and SHA-256 [163] hash of the file that contains the rules. An alternative approach to implementing the rules would be to store them within the *te:RuleBook* individual.

11.7 Participant

The predicate *Participant* was specified in Section 7.5. It is modelled as an OWL class. Section 11.7.1 gives the requirements for the Participant class, which is defined in Section 11.7.2.

11.7.1 Prerequisites

11.7.1.1 Name and unique identification

It must be possible to name things, including participants. For this purpose a data property *te:name* is created. However, it is assumed names might not be unique, and all individuals in the $\mathcal{TE}$ data model need to be uniquely identified. Identifier uniqueness is achieved by using a specific attribute, linked via the property *identifiedBy*. An alternative would be to use a combination of attributes; indeed using more attributes may provide more flexibility. However, such flexibility would not add value to the current implementation, and so a single attribute is used.

To guarantee uniqueness, the identity of a participant is expressed via an individual identifier of class of *te:ID* and related to the participant via *identifiedBy*. This identifier is uniquely attributed because it is based on the functional property *identifiedBy*. For functional properties, the reasoner's consistency checks ensure that it has only been allocated once (and tools such as data modellers and database systems refuse to allocate more than one value). The *te:ID* individual has a functional data property, *te:uniqueText*, where a unique value is registered.

The issuer of this identifier is registered through the object property *prov:wasAttributedTo*.

11.7.1.2 Natural Person or Organisation

A participant[11] can be a natural person or an organisation. The latter may or may not be a legal person.

- For natural persons, the class *te:LivingThing* is created as the basis for all living things. The class *te:NaturalPerson* is defined as equivalent to a *te1:LivingThing* that has a name.
- For organisations, the W3C Organization ontology[12] is used.
- For legal persons, the class *te:LegalPerson* is created.

The definition of participant should indicate whether it is a *te:NaturalPerson* or an *org:Organization*.

11.7.1.3 Rulebook and agreement

The class *te:RuleBook* allows individual rulebooks to be created. The object property *te:doesAgreesTo* allows a participant to express its agreement to interact according to a rulebook.

11.7.2 Participant class

The class *te:Participant* is defined as equivalent to the union of *te:NaturalPerson* and *org:Organization*, and identification is available from *te:ID*. Identity uniqueness is achieved by relating the participant to an individual of the class *te:ID*. Individuals that meet the criteria will automatically be classified by the reasoner as *Participant*. In Protégé, the Hermit reasoner will ensure this, and when the data is loaded into the back-end database the GraphDB reasoner takes care of this.

The object property *prov:wasAttributedTo* is used to record the source of the identity attribution. For a self-attested identity, the *te:ID* individual is linked to the source participant, which is the same as the subject of the identified participant. For object properties, both

[11] The data model defined in Chapter 7 includes the actor predicate. Evaluation of trustworthiness requires that actors qualify as participants. As a consequence there is no need to implement the actor class, since the evaluation is only concerned with participants.

[12] W3C makes use of the American spelling

prov:wasAttributedTo and *doesIdentify* link the *te:ID* individual to the same participant. Figure 11.1 shows a partial $\mathcal{TE}$ graph, focused on the Participant class.

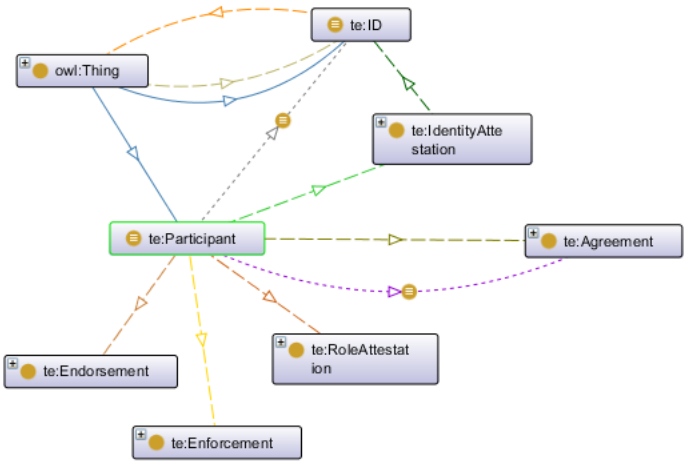

Figure 11.1: The *te:Participant* class in its context

11.8 Agreement

The predicate Agreement was specified in Section 7.7. The class and its properties are as follows.

- The class *te:Agreement* is defined to be a subclass of *te:TemporalRelation*. A specific agreement is expressed as an individual of the *te:Agreement* class.
- The object property *te:pAgreement* links[13] a participant to an agreement *(te:Participant → te:pAgreement → te:Agreement)*.
- The object property *agreementR* links an agreement to a rulebook *(Agreement → agreementR → Rulebook)*.

11.9 Endorsement

The predicate *Endorsement* was specified in Section 7.8. The class and its properties are as follows.

[13]The symbol → is used here to indicate a link, not an implication.

- The class *te:Endorsement* is defined to be a subclass of *te:TemporalRelation*. A specific endorsement is expressed as an individual of the *te:Endorsement* class.
- The object property *te:pEndorsement* links a participant to an endorsement individual (*Participant* → *te:pEndorsement* → *te:Endorsement*).
- The endorsement individual is linked to a rulebook by the object property *te:endorsementR* (*te:Endorsement* → *te:endorsementR* → *Rulebook*).
- The object property *te:pEndorsedBy* is the inverse of *te:pEndorsement*.

11.10 Enforcement

The predicate *Enforcement* was specified in Section 7.9. The class and its properties are as follows.

- The *te:Enforcement* class is defined to be a subclass of *te:TemporalRelation*.
- The object property *te:pEnforcement* relates a participant to an enforcement individual (*te:Participant* → *te:pEnforcement* → *te:Enforcement*).
- The enforcement individual is related to a rulebook by the object property *te:enforcementR* (*Enforcement* → *te:enforcementR* → *te:Rulebook*).
- The object property *te:pEnforcedBy* is the inverse of *te:pEnforcement*.

11.11 Attestations

11.11.1 Attestation

The predicate *Attestation* was defined in Section 7.4. It has the form *Attestation*(a_{id}, T), where

- a_{id} represents the actor that issued the attestation, and
- T is a triple (subject, attribute, value) where
  - *subject* identifies the actor that is the subject of the attestation,
  - *attribute* specifies the attribute that is attested by the issuer a_{id} about the subject, and
  - *value* contains the value of the attribute.

The class *te:Attestation* is defined as a subclass of *te:TemporalRelation*. Each component of the triple T is implemented as a class and its properties. The issuer a_{id} is implemented as provenance. Time and commitment marks are not implemented.

11.11.2 Identity attestation

Participant identification was specified in Section 7.5.3. It is implemented as the combination of the following:

- the unique identifier, specified in Section 11.5, and
- the class *te:IdentityAttestation*, which allows identity attestations from different issuers to be linked to an identifier.

The class *te:IdentityAttestation* is defined as a subclass of *te:Attestation*. Participants are linked to individuals of this subclass by the object property *pIdentityAttestation* with domain *Participant* and range *IdentityAttestation*. Each individual of the class *te:IdentityAttestation* is

- uniquely identified through an individual of *te:ID* and related to it via *identifiedBy*, and
- linked to the identity (*te:ID*) it attests via the property *identityAttestationId*

The issuer of an identity attestation is registered through the object property *prov:wasAttributedTo*. An identity does not need to be attested to be loaded into the OWL environment.

11.11.3 Role attestation

Roles were specified in Section 7.6. Two possible approaches to role modelling are as follows.

- A role can be to modelled directly as a class, allowing participants to be members. However, a role is a participant attribute that may vary over time. Creating a role class and making participants a member would not model the temporal aspect. A participant would either be in a role or not.
- A role can be modelled as a subclass of *te:Attestation*, allowing the relation between participants and roles to be limited in time.

The second approach was adopted for the implementation because this corresponds best to the dynamics of the real-world, which will be reflected in instance data.

The class *te:RoleAttestation* expresses that a participant is attested by the issuer of the attestation in the role referred to by the attestation. It is defined as a subclass of *te:Attestation*, which is a subclass of *te:TemporalRelation*.

The object properties *pRoleAttestation* and *roleAttestationR* have a similar role to those created for identity attestation.

The roles are specified as a set of possible roles. The role class is defined by listing its instances (AB, AS, CAB, CsSP, EnDo, EnFo, EvSP, FuSC, FuSP and TwsMo).

The issuer of a role attestation is registered through the object property *prov:wasAttributedTo*.

11.11.4 Norm

As specified in Section 6.5.1, the terminology defined in ISO/IEC 17000:2020 [173] is used for accreditation and conformity assessment. According to this standard, 'Specified requirements can be stated in normative documents such as regulations, standards and technical specifications.' To allow accreditation and conformity assessment to express such a reference to a normative document, the class *te:Norm* is defined. An individual of this class represents a norm.

- The class *te:Norm* is defined as a subclass of *owl:Thing*.
- The author of a norm is registered through the object property *prov:wasAttributedTo*.
- The class *te:Norm* has two subclasses:
  - *te:Standard*, which specifies a standard from a recognised standards organisation. An entity is linked to a standard through a conformance attestation. This is described in Section 11.11.6.
  - *te:LegalNorm*, which specifies a document from a recognised legal source. An entity is linked to a legal norm through a legal qualification attestation. This is described in Section 11.11.9.
- The data property *te:NormURI* links a norm to the URI where the norm is published.

11.11.5 Accreditation

The class *te:Accreditation* expresses that a participant is accredited, to the specified norm, by the issuer[14]. The class and its related properties are as follows.

- The class *te:Accreditation* is defined to be a subclass of *te:Attestation*.
- The issuer of an accreditation assertion is registered through the object property *prov:wasAttributedTo*.
- The object property *te:pAccreditation* links a participant to an accreditation individual (*Participant* → *te:pAccreditation* → *te:Accreditation*).
- The accreditation individual is linked to a norm by the object property *te:accreditationN* (*te:Accreditation* → *te:accreditationN* → *te:Norm*).

[14] A rulebook may specify restrictions on the issuer, e.g. it may be required that the issuer is an accreditation body.

11.11.6 Conformance

The class *te:Conformance* expresses that a participant is conformity assessed, to the specified norm, by the issuer[15]. The class and its related properties are as follows.

- The class *te:Conformance* is defined to be a subclass of *te:Attestation*.
- The issuer of a conformance assertion is registered through the object property *prov:wasAttributedTo*.
- The object property *te:pConformance* links a participant to a conformance individual (*Participant → te:pConformance → te:Conformance*).
- The object property *te:aConformance* links an attestation to a conformance individual (*Attestation → te:aConformance → te:Conformance*).
- The conformance individual is linked to a standard by the object property *te:conformanceN* (*te:Conformance → te:conformanceN → te:Norm*).

11.11.7 Supervision

The class *te:Supervision* expresses that a participant is supervised by another participant. The class and its related properties are as follows.

- The class *te:Supervision* is defined to be a subclass of *te:Attestation*.
- The issuer of a supervision assertion is registered through the object property *prov:wasAttributedTo*.
- The object property *te:pSupervision* links a participant to a supervision individual (*Participant → te:pSupervision → te:Supervision*).
- The supervision individual is linked to a another participant by the object property *te:supervisionP* (*te:Supervision → te:supervisionP → te:Participant*).

11.11.8 Registration

The class *te:Registration* expresses that a participant is registered in a registry. The class and its related properties are as follows.

- The class *te:Registration* is defined to be a subclass of *te:Attestation*.
- The issuer of a registration assertion is registered through the object property *prov:wasAttributedTo*.

[15] A rulebook may specify restrictions on the issuer, e.g. the issuer may be required to be a conformity assessment body.

- The object property *te:pRegistration* links the participant that is the subject of the registration to a registration individual (*Participant* → *te:pRegistration* → *te:Registration*).
- The data property *te:RegisterURI* links the registration to the URI where the registered subject's registration is published.

11.11.9 Legal qualification

The class *te:LegalQualification* expresses that a participant is legally qualified according to the issuer. The class and its related properties are as follows.

- The class *te:LegalQualification* is defined to be a subclass of *te:Attestation*.
- The issuer of a legal qualification assertion is registered through the object property *prov:wasAttributedTo*.
- The object property *te:pLegalQualification* links the participant that is the subject of the qualification to a qualification individual (*Participant* → *te:pLegalQualification* → *te:LegalQualification*).
- The qualification individual is linked to a norm by the object property *te:legalQualificationN* (*te:LegalQualification* → *te:legalQualificationN* → *te:Norm*).
- The object property *te:raLegalQualification* links the role attestation that is the subject of the qualification to a qualification individual (*RoleAttestation* → *te:raLegalQualification* → *te:LegalQualification*).

11.11.10 Disclosure

The class *te:Disclosure* expresses that a participant discloses information at a location that is specified as a URI. The class and its related properties are as follows.

- The class *te:Disclosure* is defined to be a subclass of *te:Attestation*.
- The issuer of a disclosure assertion is registered through the object property *prov:wasAttributedTo*.
- The object property *te:pDisclosure* links the participant that discloses the information to a disclosure individual (*Participant* → *te:pDisclosure* → *te:Disclosure*).
- The data property *te:DisclosureURI* links the disclosure to the URI where the disclosure is published.

11.12 Data sources

The class *te:DataSource* represents a source of information that can be used to bind variable occurrences in predicates. The class and its related properties are as follows.

- The class *te:DataSource* is defined to be a subclass of *owl:Thing*.
- Properties from the provenance ontology are used to describe the class as follows.
  - The entity responsible for a data source (a_{id}) is registered through the object property *prov:wasAttributedTo*.
  - The location (URI) where the data source can be accessed is registered through the object property *prov:atLocation*, and
  - The activity performed by the responsible to make the data source available (*howPublished*) is registered through the object property *prov:wasGeneratedBy*.

11.13 Overview

11.13.1 Classes

Figure 11.2 shows the graph of $\mathcal{TE}$ top-level classes as represented in Protégé's OntoGraph explorer.

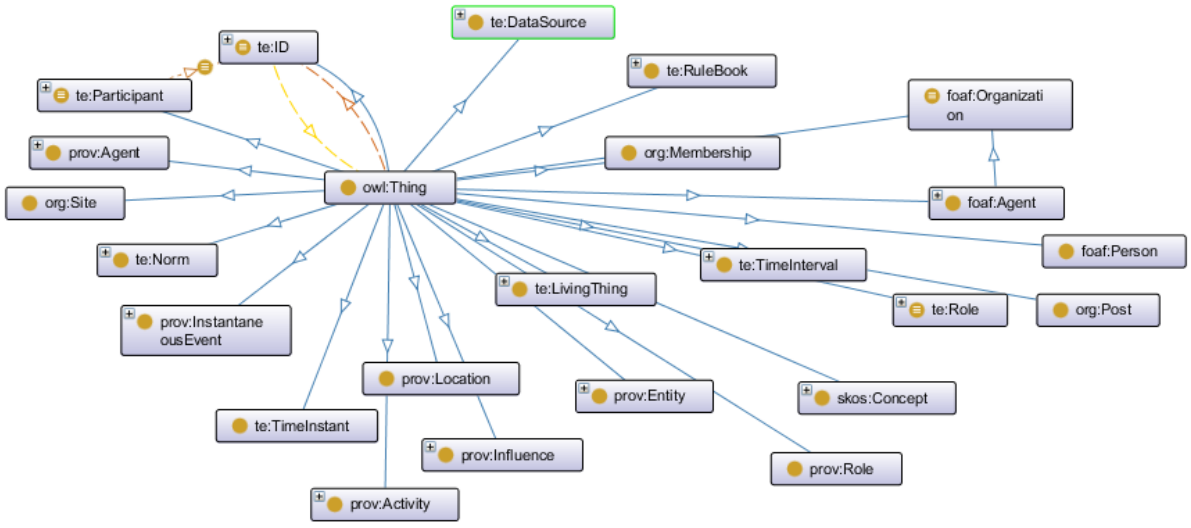

Figure 11.2: Overview of the $\mathcal{TE}$ top-level classes.

11.13.2 Object properties

Figure 11.3 shows the $\mathcal{TE}$ object properties in Protégé 's property explorer.

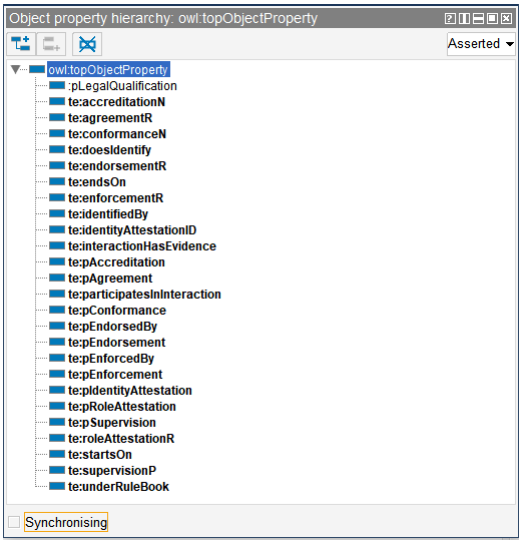

Figure 11.3: Overview of the $\mathcal{TE}$ object properties.

11.13.3 Data properties

Figure 11.4 shows the $\mathcal{TE}$ data properties in Protégé 's property explorer.

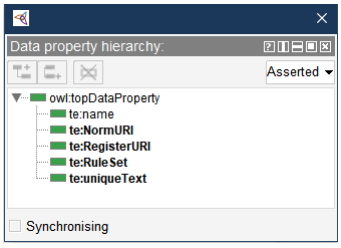

Figure 11.4: Overview of the $\mathcal{TE}$ data properties

11.14 Summary

This chapter described how the data model that was specified in Chapter 7 has been implemented in OWL DL. The resulting ontology is available at `http://www.marcsel.eu/onto/te/te-data-model.owl`. The approach to developing the implementation was described and can be summarised as follows. The ontology was created by specifying the classes and properties that implement the predicates that were specified in Chapter 7. Where relevant, classes

and properties from existing ontologies were reused; otherwise, new ones were defined. The set-up of Protégé, the tool that was used as data modeller, was described, as well as how each of the predicates were modelled. An overview of the classes and properties used was provided as shown in the Protégé tool.

Chapter 12

Implementation of data import and transformation

This chapter presents an implementation of mechanisms for the transformation of instance data, and its import into the data repository described in the previous chapter. This includes the selection of data sources, the download of data, its transformation into the format required by the $\mathcal{TE}$ data model, and the addition of provenance information. A description is also provided of how the transformed data was integrated and loaded into a graph database.

12.1 Introduction

The first step in demonstrating the practical feasibility of the proposed solution involved the implementation of the data model (see Chapter 11). To be of practical use, the evaluation functions must have access to relevant data, the issue addressed in this chapter.

Authoritative data sources were selected that provide instance data corresponding to the predicates specified in Chapter 11. Data was downloaded from those sources, transformed, tagged with provenance information, integrated and loaded in a local repository.

An implementation of this process is described in this chapter. The implementation includes all the steps from selection to downloading, but is partial because it is limited in terms of the data sources that were used and the amount of data that was downloaded. The remainder of the chapter is structured as follows

- Section 12.2 presents the approach that was used for selection, download, transformation and integration of data, and Section 12.3 describes the technical set-up.
- Section 12.4 covers the creation of data sources for organisations.

- Section 12.5 covers the creation of trustworthiness monitors and evidence service providers on the basis of public trusted lists.
- Section 12.6 covers the creation of an additional trustworthiness monitor and of identity and role attestations on the basis of the public European List of Trusted Lists.
- Section 12.7 covers the creation of accreditation bodies and conformity assessment bodies.
- Section 12.8 covers the creation and attestation of participants based on norms. This covers the use of legislation and standards.
- Section 12.9 covers the creation and attestation of organisations based on public company data.
- Sections 12.10 and 12.11 cover endorser and enforcer.
- Sections 12.12, 12.13 and 12.14 cover the creation of natural persons.
- Section 12.15 describes additional self-attestations.
- Section 12.16 covers data integration. It describes how the files created in the preceding sections were combined to form a single file, suitable for loading into a semantic web tool.

A summary is provided in Section 12.17.

12.2 Approach

To create the partial implementation, the following steps were performed for the data elements that represent predicates stored in the repository, each of which is examined in greater detail immediately below:

- selection of authoritative data sources that provide instance data corresponding to the predicates specified in the data model;
- data download from those sources;
- data transformation and tagging with provenance information;
- data loading into a local GraphDB repository.

12.2.1 Selection of data sources

12.2.1.1 Data source selection criteria

There are many data sources that contain data related to one or more predicates. Requirement IR7 'Obtaining credible data' is relevant to the selection of sources. It is specified in Section 5.5.7 in the following way.

As a participant in an electronic ecosystem I can understand the origin and the type of data that is used in the evaluation of trustworthiness of participants, so that I can claim the outcome of the trustworthiness evaluation is based on credible data.

To meet this requirement, Section 10.2.3.1 gives the following criteria for a data source and its data.

- The data source must make relevant data available, i.e. data specified in the data model. This means that the data from the data source must be mappable to one or more predicates specified in the $\mathcal{TE}$ data model.
- The data source must be authoritative for this data. Where possible data sources that are legally qualified as authoritative for the provided information must be used.
- The data must include a description of its meaning.
- The data must be available in a machine readable format. If the data is also available in a human readable format, this is additionally valuable.

12.2.2 Data download

There are at least two ways to make data available to the evaluation algorithms:

- via downloading, and
- via on-line access.

The implementation we describe here uses downloading. The data downloading step is represented as the building block 'Extract and transform' in Figure 10.1. The data must be extracted from the data sources without modification. The downloaded data is transformed according the $\mathcal{TE}$ data model and provenance information is added. Possible implementations using on-line access are left for further research.

12.2.3 Data transformation and tagging

The information in the sources we used is not structured according to the data model described in Chapter 11. It was therefore necessary to transform the data into the format of the $\mathcal{TE}$ data model. The mapping from data source information to the $\mathcal{TE}$ data model and the transformation is described below. Provenance information about data source and transformation logic was added as described in Section D.2.2.2. All the programs used to perform data transformation are available online[1].

12.2.4 Data loading

After transformation, the data was loaded without modification into a repository, making it available to the evaluation functions.

12.3 Set-up

There was no specific set-up required for data source selection as it involved manual inspection of the candidate data sources and application of the selection criteria. For the selected data sources, the download was performed in the simplest way possible. This is described individually for each data source. The set-ups for transformation and loading are described immediately below.

12.3.1 Transformation

12.3.1.1 Components

An Eclipse development environment was used, as described in Section 10.3.3. Background to the implementation of the transformations is provided in Appendix F.6.

12.3.1.2 Location

The implementation source and data files were stored locally on a Personal Computer in an Eclipse project under the name TI (TE Integration). The following subdirectories were used.

- */xml* contains the downloaded XML input files.
- */pdf* contains the downloaded PDF input files.
- */xsl* contains the XSL transformation programs.

[1] They can be accessed at `http://www.marcsel.eu/ti/xsl/NAME.xsl` where NAME should be replaced with the name of the desired transformation

- */src* contains the source code of the Java programs that execute the transformations.
- */log* contains the log files of the executions.
- */rdf* contains the resulting RDF files.

12.3.2 Loading

12.3.2.1 Components

The transformed data was loaded into a GraphDB database following the relevant documentation [266]. A repository was created with OWL Max[2] as its rule-set. The base url `http://www.marcsel.eu/onto/te/` was specified. Data was loaded into the repository using the *import RDF* function. Loaded data can be used in two ways.

- It can be interacted with via the GraphDB Workbench. This allows interactive creation and execution of queries, as well as storage and retrieval of queries and their results.
- It can be interacted with programmatically, using a program that implements a RDF4J[3] client. RDF4J is an open source Java framework for working with RDF data. It allows parsing, storing, inferencing and querying of such data through an API that connects with a SPARQL endpoint.

The GraphDB Workbench was used to develop and execute all queries. Whilst not the approach adopted, RDF4J appears to offer helpful features for accessing and integrating data sources online; its use remains an area for possible future research.

12.3.2.2 Naming conflicts

The data that resulted from the transformations was analysed both in Protégé and in GraphDB. There were some minor differences as to how IRIs were interpreted by the tools' parsers, occasionally resulting in errors.

The cause of these errors was usually the use of blanks or underscores in IRIs. This was because many IRIs were generated from public data sources. In those cases, blanks and underscores were replaced by dashes ('-').

12.4 Data sources for organisations

A range of public data sources were considered for use, and those adopted are listed below. We restrict our attention here to data sources for organisations (data sources for natural person

[2] Introduced in Section 10.3.4.1
[3] See `https://rdf4j.org/`

were addressed in Section 12.12). Data sources should preferably be authentic sources for the information they provide. The role of an authentic source is described in Section 6.5.1 as a participant that holds a mandate to register and validate information about entities. This information, or part thereof, is then made available under its responsibility. Authentic sources have been established in a variety of ways.

Two obvious possibilities for sourcing organisation data, namely the Domain Name System (DNS) and TLS certificates were considered but rejected, as in neither case do they relate directly to organisations (the DNS provides unique names for websites on the Internet, and TLS certificates relate to specific domains which, although they may belong to an organisation, do not correspond to the organisation as a whole).

An initial review of further potential data sources led to the following candidates:

- the Trusted Lists that were implemented as part of the eIDAS Regulation [103] implementation;
- the List of Trusted Lists that was implemented for the same purpose;
- membership lists of the European Accreditation association and the national accreditation organisations;
- company data published by the Global Legal Entity Identifier Foundation (GLEIF) and other officially mandated organisations such as Central Banks;
- self-published information.

For each candidate data source, the possible data items that could be mapped onto predicates were identified, and the selection criteria specified in Section 12.2.1 were applied. Where this application led to the conclusion that the use of the data source was justified, a download and transformation mechanism was established. This process is next described for each individual data source.

12.5 Organisations based on TL data

The European trusted lists were established as part of the implementation of the eIDAS Regulation [103], which included the organisation of a European scheme of trusted lists[4] published by national Trusted List Scheme Operators (TLSOs). Background information on, and a description of, the technical aspects of trusted lists are provided in appendix F.

[4]Following common practice, we use the terms trusted list and trust list interchangeably. The defining specification, ETSI TS 119 612 [89] uses the term 'Trusted Lists', and this is also used here.

12.5.1 Mapping

Since the TL information is not available in the $\mathcal{TE}$ data model format, a transformation is required. Therefore a mapping is necessary between the $\mathcal{TE}$ data model and the description of the trusted list.

- For the $\mathcal{TE}$ data model, the description from Chapter 7 was used.
- For the trusted list information, the description from ETSI TS 119 612 [89] was used.

A comparison of these descriptions led to the conclusion that the following mapping can be used.

- The TLSO which issued the trusted list, identified by <*tsl:SchemeOperatorName*>), corresponds to a trustworthiness monitor in the $\mathcal{TE}$ data model. The 'Quality and Safety' department of the Belgian Federal Public Service (FPS) Economy, SMEs, Self-employed and Energy is an example of a Belgian TLSO.
- The TSP that delivers trust services, identified by <tsl:TrustServiceProvider>), corresponds to an evidence service provider in the $\mathcal{TE}$ data model.

12.5.2 Trusted lists as data sources

12.5.2.1 Application of selection criteria

As shown in Table 12.1, trusted lists meet the selection criteria defined in Section 12.2.1. They are relevant data sources for trustworthiness monitor and evidence service provider predicates. To adhere to the requirements IR2 (transparency) and IR7 (data source credibility) the provenance of the information used to bind variable occurrences must be included. As a consequence, all usage of a TL as data source needs to refer to the original source. $\mathcal{TE}$ data sources that include a link to the original TL source were created for this purpose. For the implementation, trusted lists issued by Belgium, Spain and the UK were used as data sources.

12.5.2.2 Transformation approach

Trusted lists are published in two formats, PDF and XML. Neither format can be loaded into the GraphDB repository because it requires use of a semantic web format such as OWL, in a syntax such as XML/RDF. Of the two formats, the XML version appears to be simplest to transform. Three common transformation approaches are compared in Appendix F.5:

- XSLT and XPath,

Selection criteria	Description
Authoritative source	TLs are provided by a Competent Authority of a Member State of the EU
Transparency	TLs are published by the European Commission in their List of Trusted Lists, available at `https://ec.europa.eu/tools/lotl/eu-lotl.xml`
Description of meaning available	The TLs themselves and all data elements within them are described in ETSI TS 119 612 [89]
Machine readable/human readable	TLs are published in machine readable XML Schema Description (XSD) format and in PDF format
Mapping possibility	Data elements can be mapped via XSLT
Respect for GDPR [101]	There is no personal information in TLs

Table 12.1: Selection criteria for data sources applied to Trusted Lists

- Jena, and
- SPIN.

On the basis of this comparison, the combination of XSLT and XPath was selected.

12.5.2.3 Trusted list download and transformation

For each of the selected trusted lists, a copy of the machine-readable version was downloaded from the location where it is published by the issuing TLSO. The locations were verified against the locations included in the LOTL and found to match.

For each downloaded trusted list, a *TL2RDF_XX_DataSource_TL_v301.xsl* program[5] was developed to create a $\mathcal{TE}$ framework data source on the basis of a trusted list file. The program combines $\mathcal{TE}$ data model predicates and provenance assertions. The $\mathcal{TE}$ data model predicates describe the data source. The following assertions describe its provenance:

- the activity (*prov:Activity*) that created the data source, including the time when the activity was performed (*prov:startedAtTime* and *prov:endedAtTime*),
- the original source (*prov:wasDerivedFrom*) of the data, i.e. the URI of the trusted list,
- the agent to which the creation of the data source can be attributed, for which a reference to `http://www.marcsel.eu/onto/ti` was used, referring to the $\mathcal{TE}$ framework's software[6]

[5] 'XX' is a placeholder for the country identifier

[6] The 'ti' refers to the '$\mathcal{TE}$ framework integration' software.

The XSL program performs the following two steps.

- The first step is the creation of the Activity individual that generates the data source. This involves the following sub-steps:
  - the creation of a resource (*'rdf:about'*) with hardcoded name based on the *xsl* program and its execution date, i.e. *http://www.marcsel.eu/ti/xsl/TL2RDF_BE_DataSource_TL_v301.xsl.2021-01-06*,
  - casting into *prov:Activity*,
  - addition of:
    - *prov:startedAtTime*, and
    - *prov:endedAtTime*.
- The second step is the creation of the DataSource individual, involving:
  - the creation of a resource with a hardcoded name based on the URI from where the trusted list file was originally obtained,
  - casting into the type of *te:DataSource*,
  - addition of *prov:wasDerivedFrom* the trusted list URI, where the TLSO published the TL,
  - addition of *prov:wasAttributedTo http://www.marcsel.eu/onto/ti*,
  - addition of *prov:wasGeneratedBy* using the activity which was created in the first step.

Each program was executed to create a corresponding *DataSource* individual. As an example, the source code of the *TL2RDF_BE_DataSource_TL* transformation and the corresponding Java driver program can be found in Listings K.1 and K.2. The output of the transformations was integrated into the database load file, as described in Section 12.16.

12.5.3 Creation of trustworthiness monitor

12.5.3.1 Input

The individual TLs were downloaded in XML format from the location where they are published by the issuing TLSO. The locations were verified against the locations included in the LOTL[7] and found to match.

[7] At the following locations:

- Belgium: `https://tsl.belgium.be/tsl-be.xml`,

12.5.3.2 Transformation and output

The transformation *TL2RDF_XX_TwsMo* creates a trustworthiness monitor individual in RDF/XML on the basis of a trusted list, issued by a TLSO, identified by the <*tsl:SchemeOperatorName*> element. As described in Section 10.3.3, an Eclipse development environment was used; technical background is provided in Appendix F.6. Provenance was added to each element in the following way.

- The property *prov:wasDerivedFrom* was added, with value the URI where the TLSO published the TL.
- The property *prov:wasAttributedTo* was added, with value the name of the TLSO that issued the TL.
- The property *prov:wasGeneratedBy* was added, with value the name of the XSL program that created the RDF/XML data source individual.

A transformation involves the following steps.

- Creation of identity individuals for the TwsMo, the TwoMo attestations, and the provenance of the TwsMo, its identity attestation, and its attestation as a TwsMo.
- Creation of attestation individuals with provenance for identity and role attestations.
- Creation of the TwsMo individual with provenance on the basis of the TL TLSO and with the allocation of the individual's identity and role attestations.

As an example, the source code of the *TL2RDF_BE_TwsMo_TL_v301.xsl* transformation can be found in Listing K.3.

The output of the transformations was saved in individual RDF files. These files were integrated into the database load file as described in Section 12.16.

12.5.4 Creation of evidence service providers

12.5.4.1 Input

The input files that were used for the creation of trustworthiness monitors, as described in Section 12.5.3, were also used to create evidence service providers.

- Spain: `https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml`,
- United Kingdom: `https://www.tscheme.org/sites/default/files/tsl-uk0022signed.xml`

12.5.4.2 Transformation functionality

The transformation *TL2RDF_XX_EvSP* creates evidence service provider individuals in RDF/XML on the basis of a trusted list, issued by a TLSO, identified by the <*tsl:SchemeOperatorName*> element. Provenance was added to each element in the following way.

- The property *prov:wasDerivedFrom* was added, with value the URI where the TLSO published the TL.
- The property *prov:wasAttributedTo* was added, with value the name of the TLSO that issued the TL. The assertions added to the database are about EvSPs and issued by the TLSO (i.e. other-attested, not self-attested).
- The property *prov:wasGeneratedBy* was added, with value the name of the XSL program that created the RDF/XML data source individual.

The transformation involves the following steps:

- creation of identity individuals for the EvSP individuals and their identity and role attestations, with provenance;
- creation of identity and role attestations individuals, with provenance;
- creation of the EvSP individuals, with provenance.

The outputs of the transformations were saved in the corresponding RDF files. These files were integrated into the database load file as described in Section 12.16.

12.6 Organisations based on LOTL Data

An introduction to the LOTL is provided in Appendix G.

12.6.1 Mapping

As the LOTL is defined as a trusted list, the mapping described in Section 12.5.1 applies. Thus the following mapping can be used.

- The LOTL identifies the European Commission as its issuing TLSO, which corresponds to a trustworthiness monitor. This can be used to create a self-attested identity and role attestation about the European Commission as trustworthiness monitor.
- The LOTL includes descriptions of national Trusted List Scheme Operators, which correspond to trustworthiness monitors. This can be used to create identity and role attestations about these trustworthiness monitors, issued by the European Commission.

Selection criteria	Description
Authoritative source	The LOTL is provided by the European Commission and a description of the information for which it is authoritative is published in the Official Journal[8]
Transparency	Further to the publication of its description in the Official Journal, the LOTL itself is publicly available at `https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml`
Description of meaning available	LOTL has the format and meaning of TL as described in ETSI specification, both in natural language and in XML Schema Description (XSD)
Machine readable/human readable	The LOTL is published in XML and PDF formats
Mapping possibility	Can be mapped via XSLT
Respect for GDPR [101]	There is no personal information in TLs

Table 12.2: Selection criteria for data sources applied to List of Trusted Lists

12.6.2 List of trusted lists as data source

12.6.2.1 Application of selection criteria

The list of trusted lists (LOTL) is a relevant data source for attestation predicates about trustworthiness monitors. As shown in Table 12.2, the LOTL meets the selection criteria defined in Section 12.2.1.

To adhere to requirements IR2 (transparency) and IR7 (data source credibility), the provenance of the information used to bind variable occurrences must be included. As a consequence, all usage of the LOTL as a data source needs to refer to the original source. A $\mathcal{TE}$ data source that include a link to the original LOTL source was created for this purpose.

12.6.2.2 Transformation approach

The approach described in Section 12.5.2.2 is also used for the list of trusted lists.

12.6.2.3 LOTL download and transformation

A copy of the LOTL was downloaded in the same way as a trusted list, as described in Section 12.5.2.3. The location is published by the European Commission[9]. A program (called

[9] `https://ec.europa.eu/digital-single-market/en/eu-trusted-lists`

TL2RDF_DataSource_LOTL_v301.xsl) was developed that contains the same steps as those described for the trusted list program, described in Section 12.5.2.3. The main differences to the trusted list program involved changes to names of data sources, resources, and attribute types and properties.

12.6.3 Creation of EC trustworthiness monitor

12.6.3.1 Input

The LOTL was downloaded in XML format from the location[10] where it is published by the European Commission, its issuing TLSO.

12.6.3.2 Transformation and output

The transformation TL2RDF_LOTL_1_v301.xsl creates a trustworthiness monitor individual on the basis of the LOTL. The issuing TLSO is identified by the <*tsl:SchemeOperatorName*> element. This TLSO, i.e. the European Commission, signs the LOTL. Provenance was added as described in Section 12.5.3.2. The transformation involves the following steps:

- creation of identities:
  - creation of an identity for the European Commission (EC) individual;
  - creation of an identity for the EC identity self-attestation;
  - creation of an identity for the EC role self-attestation.
- Attestations:
  - creation of an EC identity self-attestation;
  - creation of an EC role self-attestation,
- Creation of the EC individual.

The XSL transformation program is available online[11]. The output of the transformation was saved to the corresponding RDF file. This file was integrated into the database load file as described in Section 12.16.

[10] `https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml`
[11] `http://www.marcsel.eu/ti/xsl/TL2RDF-LOTL-1-v301.xsl`

12.6.4 Creation of identity and role attestations

12.6.4.1 Input

The input file described in Section 12.6.3 was used for the creation of role and identity attestations.

Note that creating the identity attestations does not create the actual individual, nor does it allocate the properties to these individuals. That is done in the respective XSLs that create the evidence service provider individuals.

12.6.4.2 Transformation and output

The transformation *TL2RDF_LOTL_2_v301.xsl* creates identity and role attestations on the basis of the LOTL. Provenance was added as described in Section 12.5.3.2. The transformation involves the following steps:

- creation of identifiers for identity and role attestations,
- creation of identity and role attestation with EC as issuer,
- relating the attestations to their own identities,
- relating the attestations to the identities they attest.

The output of the transformation was saved in the corresponding RDF file. This file was integrated into the database load file as described in Section 12.16.

12.7 Attestations based on accreditation

12.7.1 Mapping

12.7.1.1 Available data

There are at least two types of organisations that provide accreditation:

- National Accreditation Bodies (NABs), mutually recognising one-another through bodies such as the European co-operation for Accreditation (EA), and
- Membership-based organisations such as the Kantara Initiative.

National Accreditation Bodies (NABs) and the European co-operation for Accreditation (EA) publish information about officially-recognised accreditation bodies. Those organisations publish information about their credentials for operating as accreditation bodies, as well as

which conformity assessment bodies (CABs) they recognise. In the case of NABs, there is a national law in each country that specifies the NAB's role.

Organisations such as the Kantara Initiative[12] are recognised by their members for their organisation of an accreditation scheme. They operation is characterised by policies, procedures and ByLaws. Members confirm their acceptance thereof when signing the membership agreement.

A selective overview of the organisation of accreditation is provided in Appendix H.

12.7.1.2 Used mapping

The role of accreditation body and conformity assessment body in the $\mathcal{TE}$ framework was described in Section 6.5.1. An analysis of the available data led to the following mapping:

- NABs correspond to $\mathcal{TE}$ data model accreditation bodies;
- NABs publish data about organisations that correspond to $\mathcal{TE}$ data model conformity assessment bodies.

The EA facilitates mutual recognition between the NABs, and is an additional source of data about them.

12.7.2 Accreditation data as data source

12.7.2.1 Application of selection criteria

As described in Table 12.3, the accreditation data meet the selection criteria defined in Section 12.2.1. The main points can be summarised in the following way.

- Accreditation data are relevant data sources for accreditation body and conformity assessment body predicates.
- NABs are legally appointed in their role. Furthermore the EA publishes an authoritative list of NABs.
- NABs publish authoritative lists of conformity assessment bodies.
- As the landscape of NABs is already broad, it was decided to limit the scope for the implementation to officially appointed NABs. Accreditation organised by membership organisations is left for further research.

[12]The Kantara Initiative Inc is a US registered 501(c) (6) tax exempt non-profit Industry Association with the goal of promoting interoperable trust.

Selection criteria	Description
Authoritative source	The NABs are authoritative because they are the competent and legally recognised authorities for accreditation within their jurisdiction. The EA is authoritative on the basis of mutual recognition by the NABs.
Transparency	The NABs and the EA publish data about their competence, their operating procedures and the standards they apply.
Description of meaning available	The terminology used in the publications is plain and understandable. The terminology used by NABs and the EA is based on the ISO/IEC 17011:2017 [174].
Machine readable/human readable	The information is published on web pages in HTML and in publicly available documents in PDF format
Mapping possibility	Data elements can be mapped manually
Respect for GDPR [101]	No personal information is published

Table 12.3: Selection criteria for data sources applied to accreditation body data

To adhere to requirements IR2 (transparency) and IR7 (data source credibility), the provenance of the information used to bind variable occurrences was included. As a consequence, all usage of accreditation data as data source can refer to the original source. $\mathcal{TE}$ data sources that include a link to the original source were created for this purpose. For the implementation, the NABs of Belgium, Spain and the UK were used, as well as the EA.

12.7.2.2 Creation of the data sources

As data is published in web pages and in PDF documents, either dedicated transformations must be developed or the OWL statements must be created manually. As the layouts of the web pages and the documents are not standardised, it was decided to manually create OWL statements on the basis of the publicly available information.

It was decided not to download the public information but to refer to the on-line information, and to manually create $\mathcal{TE}$ data sources and AB and NAB statements with references to this on-line information. The following data sources were created, containing the information described in Section 12.5.2.3.

- To use the Belgian NAB as a data source, the OWL file *PDF2RDF-DataSource-BELAC-v301.rdf* was created. It uses the on-line Royal Decree[13] that established BELAC as name

[13] `https://economie.fgov.be/sites/default/files/Files/Publications/files/Belac-NL/`

for the data source.

- To use the United Kingdom's NAB as a data source, the OWL file *PDF2RDF-DataSource-UKAS-v301.rdf* was created. It uses the on-line Accreditation Regulations 2009[14] that established the UKAS organisation as name for the data source.
- To use the Spanish NAB as a data source, the OWL file *PDF2RDF-DataSource-ENAC-v301.rdf* was created. It uses the on-line Royal Decree[15] that established the ENAC organisation as name for the data source.
- To use the EA as a data source, the OWL file *PDF2RDF-DataSource-EA-v301.rdf* was created. It uses the on-line Regulation[16] that appointed the EA in its role as name for the data source.

As these data source individuals were created manually as part of the implementation, they were attributed to `http://www.marcsel.eu/onto/ti`.

12.7.3 Creation of accreditation bodies

12.7.3.1 Using NAB data

As an example, we next describe how BELAC is created as a $\mathcal{TE}$ data model AB. A query on the BELAC website identified the legal act[17] which established the organisation. The implementation of the *te:Norm* that models this act was described in Section 12.8.4. To create the Belgian NAB as a $\mathcal{TE}$ data model AB, the file *PDF2RDF-AB-BE-BELAC-v301.rdf* was created. This was done in a similar way to that described in Section 12.5.3, and can be summarised as follows.

- The URI of the on-line Royal Decree[18] that established BELAC was used to refer to the data source on which the AB individual and its attestations are based.
- Identifiers for the BE-BELAC individual and its identity, role and legal attestations were created.
  - Identity was justified on the basis of the information published by the data source[19].

0-05-NL.pdf

[14] `https://www.legislation.gov.uk/uksi/2009/3155/pdfs/uksi_20093155_en.pdf`

[15] `https://www.boe.es/buscar/pdf/2011/BOE-A-2011-398-consolidado.pdf`

[16] `http://data.europa.eu/eli/reg/2008/765/oj`

[17] `https://economie.fgov.be/sites/default/files/Files/Publications/files/Belac-NL/0-05-NL.pdf`

[18] `https://economie.fgov.be/sites/default/files/Files/Publications/files/Belac-NL/0-05-NL.pdf`

[19] At `https://economie.fgov.be/nl/themas/kwaliteit-veiligheid/accreditatie` BELAC is declared as part of the Federal Public Service Economy.

– The AB role was justified on the basis of the information published by the data source[20].

- The BE-BELAC individual was created and cast into the types *org:Organization* and *prov:Organization*, and linked to its identity, role and legal qualification attestations. It was created manually as part of the implementation. As a consequence it was attributed to `http://www.marcsel.eu/onto/ti`.

In a similar way, individuals that implement the French and UK accreditation bodies were created. The files *PDF2RDF-AB-BE-BELAC-v301.rdf*, *PDF2RDF-AB-FR-COFRAC-v301.rdf*, *PDF2RDF-AB-UK-UKAS-v301.rdf* and *DBLN.owl* were integrated into the database load file as described in Section 12.16. Figure 12.1 shows the BELAC accreditation body and its properties as displayed by the explorer utility of GraphDB.

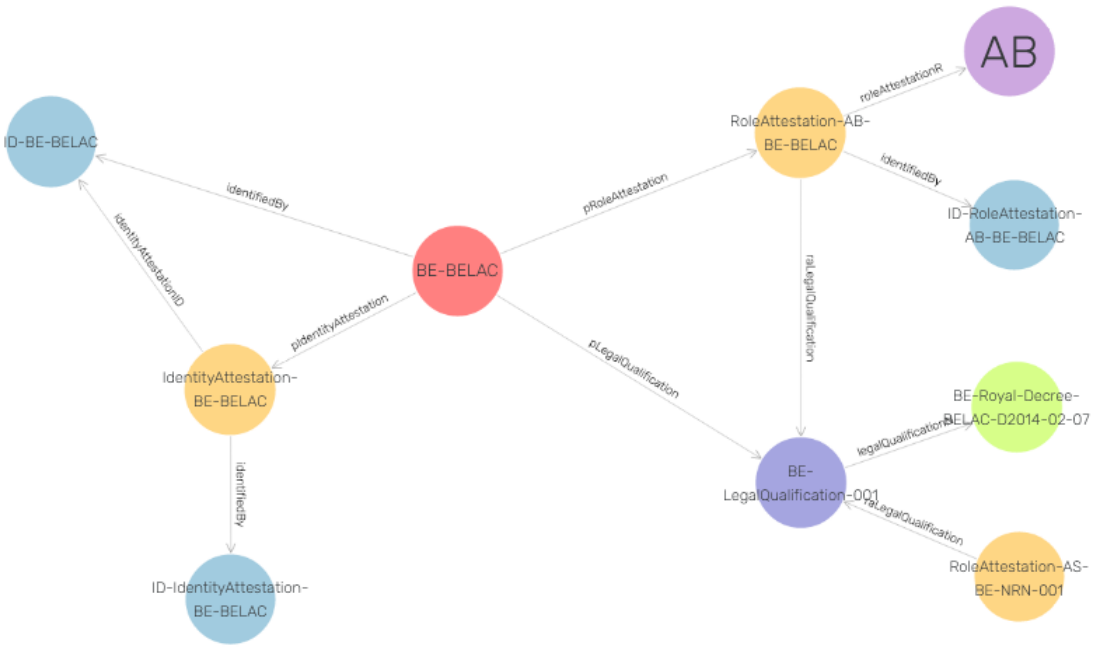

Figure 12.1: BELAC accreditation body and its properties

12.7.3.2 Using EA data

Identity and role attestations can be created on the basis of the data provided by the EA[21]. EA-based attestations can be created following a similar approach to that used for NAB-based

[20] At `https://economie.fgov.be/sites/default/files/Files/Publications/files/Belac-NL/1-01-NL.pdf` BELAC is declared as accreditation body.

[21] `https://european-accreditation.org/ea-members/directory-of-ea-members-and-mla-signatories/`

attestations.

12.7.4 Creation of conformity assessment bodies

Accreditation data from three NABs was used to create CABs:

- BELAC, the Belgian Accreditation Body,
- COFRAC, the French Accreditation Body, and
- UKAS, the United Kingdom Accreditation Body,

12.7.4.1 BELAC derived CABs

The accreditation data used to create CAB individuals needs to describe the CABs and for which standards they are accredited, i.e. standards to which they are allowed to assess the conformance of their clients.

To obtain this information, the BELAC website was queried[22] by specifying 'Information Technology' as product or service; it responded that two entities were accredited as CAB for 'ISO/IEC 27001[23]':

- VINCOTTE SA/NV, and
- KPMG CERTIFICATION bv.

For both entities the provided list included the same standards:

- ISO/IEC 27001:2013 [177],
- ISO/IEC 27006:2015 [178], and
- ISO/IEC 17021-1:2015 [175].

For each standard an OWL individual of type *te:Standard* was created in the file *DBLN.owl*. For VINCOTTE SA/NV and KPMG CERTIFICATION bv, individuals of the type CAB were created in the file *PDF2RDF-BELAC-CABs-v301.rdf*. This includes the statements described in Section 12.5.3 for the inclusion of provenance and the creation of the CAB individuals, which can be summarised in the following way.

[22] `https://economie.fgov.be/nl/themas/kwaliteit-veiligheid/accreditatie-belac/geaccrediteerde-instellingen/certificatie-instellingen-van-2`

[23] The version of the standard was not mentioned, but it was mentioned on the electronic document that is displayed on the website. This document was downloaded to local storage as evidence.

- The URI of the on-line Royal Decree[24] that established BELAC was used to refer to the data source on which the CAB individuals and their attestations are based.
- Identifiers for the CAB individuals accredited by BELAC, and their identity, role and accreditation attestations were created.
- The CAB individuals accredited by BELAC, and their identity, role and accreditation attestations were created and linked to their identifiers.
  - The CAB identity attestation was justified on the basis of the information published by BELAC[25], to whom it was attributed.
  - The CAB role attestation was justified on the basis of the information published by BELAC, to whom it was attributed.
- The CAB individuals were defined and cast into the types *org:Organization* and *prov:Organization*. They were linked to their identity, role and accreditation attestations. The CAB individuals was attributed to BELAC.

The files *PDF2RDF-BELAC-CABs-v301.rdf* and *DBLN.owl* were integrated into the database load file as described in Section 12.16.

12.7.4.2 COFRAC derived CABs

The approach described in the preceding section was again followed to create CABs that are accredited by COFRAC.

The COFRAC website was queried[26] by specifying 'Information Technology' as product or service; it responded that 24 entities were accredited in this domain. A query for 'Information Security' returned 26 entities. For the implementation of the thesis, one entity was used: 'LA SECURITE DES TECHNOLOGIES DE L'INFORMATION LSTI SAS'. Its accreditation[27] statement lists a series of norms including:

- ETSI standards including ETSI EN 319 401 [90], ETSI EN 319 403 [88], ETSI EN 319 411-1 [92] and -2 [94], ETSI EN 319 421 [96],
- the standard ILNAS/PSCQ/Pr001 'Supervision of Qualified Trust Service Providers (QTSPs)' [162] from Luxembourg, and

[24] `https://economie.fgov.be/sites/default/files/Files/Publications/files/Belac-NL/0-05-NL.pdf`

[25] At `https://economie.fgov.be/nl/themas/kwaliteit-veiligheid/accreditatie` BELAC is declared as part of the Federal Public Service Economy.

[26] `https://tools.cofrac.fr/fr/easysearch/index.php`, queried on 7 February 2021

[27] `https://tools.cofrac.fr/annexes/sect5/5-0546.pdf`, queried on 7 February 2021

- specific eIDAS Regulation [103] articles including Art. 5(1), Art. 13(2), Art. 15, Art. 19(1), Art. 19(2), Art. 24(2) etc.

For the ETSI standards mentioned above, an OWL individual of the type *te:Standard* was created in the file *DBLN.owl*. For 'LA SECURITE DES TECHNOLOGIES DE L'INFORMATION LSTI SAS' an individual of the type CAB was created in the file *PDF2RDF-COFRAC-CABs-v301.rdf*. This includes the statements described in Section 12.5.3 for the inclusion of provenance.

The files *PDF2RDF-COFRAC-CABs-v301.rdf* and *DBLN.owl* were integrated into the database load file as described in Section 12.16.

12.7.4.3 UKAS derived CABs

The approach described in the preceding section was followed to create CABs that are accredited by UKAS. The UKAS website was queried[28] for the accreditation of the companies identified by tScheme as assessors. For the implementation of the thesis, three entities were used.

- Lloyd's Register,
- KPMG LLP, and
- KPMG Audit Plc.

For each assessor, an individual of the type CAB was created in the file *PDF2RDF-UKAS-CABs-v301.rdf*. This includes the statements described in Section 12.5.3 for the inclusion of provenance. KPMG Audit Plc as identified by UKAS[29] could not be found in the UK company register [30]. As a consequence, the provenance attribute *prov:wasDerivedFrom* was not allocated.

The files *PDF2RDF-UKAS-CABs-v301.rdf* and *DBLN.owl* were integrated into the database load file as described in Section 12.16.

12.7.5 Creation of evidence service providers

As a consequence of the Brexit, see Section 2.2.3.2, the United Kingdom's approach for establishing evidence service providers is independent of eIDAS. To demonstrate how this approach fits in the proposed framework, an evidence service provider from the United Kingdom has been implemented.

[28] `https://www.ukas.com/find-an-organisation/`, queried on 22 February 2021
[29] KPMG Audit Plc, One Snowhill Snowhill Queensway Birmingham B4 6GH United Kingdom
[30] `https://find-and-update.company-information.service.gov.uk/`

The company Secure Meters Limited operates a PKI service for smart meters. On the basis of the tScheme service description thereof, an evidence service provider was created using the name 'SMETS1 PKI Service from SML' in the file *PDF2RDF-UK-EvSP-tScheme-v301.rdf*. This file was integrated into the database load file as described in Section 12.16.

12.8 Attestations based on norms

Norms were introduced in Section 11.11.4, which specified the class *te:Norm*, with the subclasses *te:LegalNorm* and *te:Standard*.

12.8.1 Mapping

12.8.1.1 Available data

Various sources provide information regarding legal norms. This includes state gazettes, official journals and ad-hoc publications by legal entities. Other sources provide information regarding standards. These include the ISO and the ETSI.

12.8.1.2 Used mapping

The role of authentic source in the $\mathcal{TE}$ framework was described in Section 6.5.1. An analysis of the available data led to the conclusion that the mapping had to be done on a case-by-case basis.

12.8.2 Norms as data source

12.8.2.1 Application of selection criteria

As described in Table 12.4, norms have the potential to meet the selection criteria defined in Section 12.2.1. Selective norms that meet the selection criteria have been used for this implementation.

12.8.3 Approach for creation of norms

As norm data is published on web pages and in PDF documents, either dedicated transformations must be developed, or the OWL statements must be created manually. As the layouts of the web pages and the documents are not standardised, it was decided:

- to manually create OWL statements on the basis of the publicly available information, and

Selection criteria	Description
Authoritative source	The state gazettes, official journals and selected ad-hoc publications are authoritative because they are the legally recognised sources for legal qualifications within their jurisdiction. A legal norm is authoritative within its jurisdiction. A standard is authoritative for those that accept to comply with it.
Transparency	Such data is published on the website of its publisher.
Description of meaning available	The terminology does contain law jargon and/or technical jargon.
Machine readable/human readable	Norm information is published on web pages in HTML and in publicly available documents in PDF format.
Mapping possibility	Data elements can be mapped manually.
Respect for GDPR [101]	No personal information is published.

Table 12.4: Selection criteria for data sources applied to accreditation body data

- not to download the public information but to refer to the on-line information.

A URI was used to refer to the original source. For legislation, the European Legislation Identifier (ELI[31]) was used to refer to the legal source where possible. For standards, the URI that refers to the standard was used. All norms were attributed to the entity that published it.

12.8.4 Creation of legal norms

The following documents were used to create norms of the type *te:LegalNorm*:

- the French Royal Decree that established the COFRAC organisation as an accreditation body,
- the Belgian Royal Decree that established the BELAC organisation as an accreditation body,
- the Belgian Law that established the National Register of Natural persons (NRN) organisation as an authentic source,

[31]The ELI is a system to make legislation available on-line in a standardised format, `https://eur-lex.europa.eu/eli-register/about.html`

- the Certipost CitizenCA Certification Practice Statement that allocates the responsibility for operating the Certification Authority which issues authentication and signature certificates on behalf of the Belgian Federal Government, and
- the Belgian Law that established the Federal Public Service 'Economy, SMEs, Self-employed and Energy' as a trustworthiness monitor (in eIDAS terminology: 'Supervisory Body').

12.8.4.1 French Royal Decree COFRAC

A *te:LegalNorm* was created on the basis of the French Decree that established the COFRAC organisation in the following way.

- A query to the COFRAC website[32] identified the organisation, its founding act and its role as accreditation body.
- The description of its role was corroborated against the Decree published in the French State Gazette[33], which confirmed the name and role of COFRAC[34].
- A *te:LegalNorm* individual was defined, using the URI of this Decree as its *te:NormURI*.

12.8.4.2 Belgian Royal Decree BELAC

A *te:LegalNorm* was created on the basis of the Belgian Royal Decree that established the BELAC organisation in the following way.

- A query on the BELAC website identified the legal act[35] that established the organisation.
- This act was corroborated against the Belgian State Gazette[36], which confirmed the name and contents of the act[37] as well as the role of BELAC as accreditation body.
- A *te:LegalNorm* individual was defined, using the *URI*[38] of the legal act as its *te:NormURI*.

[32] `https://www.cofrac.fr/mentions-legales/`
[33] `https://www.legifrance.gouv.fr/`
[34] `https://www.legifrance.gouv.fr/loda/id/JORFTEXT000019992087/`
[35] `https://economie.fgov.be/sites/default/files/Files/Publications/files/Belac-NL/0-05-NL.pdf`
[36] `http://www.ejustice.just.fgov.be/`
[37] `http://www.ejustice.just.fgov.be/eli/besluit/2014/02/07/2014011058/justel`
[38] `http://www.ejustice.just.fgov.be/eli/besluit/2014/02/07/2014011058/justel`

12.8.4.3 Belgian Law NRN

A *te:LegalNorm* was created on the basis of the Belgian Law that established the NRN organisation in the following way.

- A query to the NRN website[39] identified the legal act[40] that established the organisation.
- This act was corroborated against the Belgian State Gazette[41], which confirmed the name and contents of the act, as well as the role of the NRN.
- A *te:LegalNorm* individual was defined, using the *URI*[42] of the legal act as its *te:NormURI*.

12.8.4.4 Certipost CPS

A *te:LegalNorm* was created on the basis of the Certipost CitizenCA Certification Practice Statement in the following way.

- A query to the Belgian eID PKI repository website[43] identified the Certipost CPS[44], which allocates the responsibility for operating the Certification Authority that issues authentication and signature certificates on behalf of the Belgian Federal Government to Certipost, Muntcentrum, Brussels.
- This company information was corroborated against the Belgian trust list[45], which confirmed the name and address as Certipost, Muntcentrum, Brussels, as well as the company's role as certificate service provider.
- A *te:LegalNorm* individual was defined, using the *URI*[46] of the CPS as its *te:NormURI*.

12.8.4.5 FPS Economy

A *te:LegalNorm* was created on the basis of the Belgian law that established the Federal Public Service 'Economy, SMEs, Self-employed and Energy' as a trustworthiness monitor (in eIDAS terminology: 'Supervisory Body') in the following way.

[39] `https://www.ibz.rrn.fgov.be/nl/rijksregister/reglementering/wetten-en-reglementering/`
[40] `http://www.ejustice.just.fgov.be/eli/wet/1983/08/08/1984021127/justel`
[41] `http://www.ejustice.just.fgov.be/`
[42] `http://www.ejustice.just.fgov.be/eli/wet/1983/08/08/1984021127/justel`
[43] `https://repository.eid.belgium.be/`
[44] `https://repository.eid.belgium.be/downloads/citizen/nl/CPS_CitizenCA.pdf`
[45] `https://tsl.belgium.be/tsl-be.xml`
[46] `https://repository.eid.belgium.be/downloads/citizen/nl/CPS_CitizenCA.pdf`

- A query to the website[47] of the Federal Public Service 'Economy, SMEs, Self-employed and Energy' identified the law[48] which allocates the responsibility for supervision of eIDAS trust services to itself.
- This information was corroborated against two sources:
  - the European list of trust lists[49], which confirmed the name and address of the Belgian supervisory body to be 'FPS Economy, SMEs, Self-employed and Energy - Quality and Safety';
  - the law[50], that allocates the responsibility for supervision to 'FPS Economy, SMEs, Self-employed and Energy' in Chapter 2, Art. 2 (Section 16).
- A *te:LegalNorm* individual was defined, using the *URI*[51] of the law as its *te:NormURI*.

Each legal norm was implemented as an OWL individual in the *DBLN.owl* file which was integrated into the database load file as described in Section 12.16.

12.8.5 Creation of legal attestations

For each of the legal norms defined in the preceding section, a *te:LegalQualification* individual was created and linked to the corresponding norm. The attested participants were linked to their legal qualifications via the property *te:pLegalQualification* in the file *DBLN.owl*. This file was integrated into the database load file as described in Section 12.16. .

12.8.6 Creation of standards

The following standards were used to create norms of the type *te:Standard*:

- ISO/IEC 27001:2013 [177],
- ISO/IEC 27006:2015 [178],
- ISO/IEC 17021-1:2015 [175],
- ETSI TS 119 403-2 [97],
- ETSI EN 319 401 [90],

[47] `https://economie.fgov.be/nl/themas/online/elektronische-handel/elektronische-handtekening-en`
[48] `http://www.ejustice.just.fgov.be/eli/wet/2016/07/21/2016009485/justel`
[49] `https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml`
[50] `http://www.ejustice.just.fgov.be/eli/wet/2016/07/21/2016009485/justel`
[51] `{http://www.ejustice.just.fgov.be/eli/wet/2016/07/21/2016009485/justel}`

- ETSI EN 319 403 [88],
- ETSI EN 319 403-1 [98],
- ETSI EN 319 411-1 [92],
- ETSI EN 319 411-2 [94],
- ETSI EN 319 421 [96],
- CA Browser Forum's 'EV SSL Certificate Guidelines version 1.7.1' [41].

Each standard was implemented as an OWL individual in the *DBLN.owl* file which was integrated into the database load file, as described in Section 12.16.

12.8.7 Creation of conformity attestations

The CABs that were described in Sections 12.7.4.1 and 12.7.4.2 publish conformity attestations as specified in Section 7.10.2. For the implementation, examples of conformity attestations based on publications of the CAB 'LA SECURITE DES TECHNOLOGIES DE L'INFORMATION LSTI SAS' were created. The CAB lists its attestations online[52], in PDF format, for the following evidence service providers:

- British Telecom,
- CertSIGN,
- Dhimyotis,
- E-Tugra, and
- Zetes.

For each EvSP, attestations and individuals were specified in PDF2RDF_FR_LSTI_EvSPs_v301.rdf. This led to the following observations.

- Regarding British Telecom:
  - British Telecom was identified by the CAB (LSTI, in their attestation letter) as 'BRITISH TELECOMMUNICATIONS PLC BT Centre, 81 Newgate Street London EC1A 7AJ United Kingdom', registered under no 01800000.

[52] `https://www.lsti-certification.fr/fr/telechargements/`

  - British Telecom was identified by the TLSO (tScheme, in the UK Trusted List) as 'BT Trust Services Helpdesk, PO Box 641 Cardiff, South Glamorgan, CF1 1YL, UK ', with NTRUK-1800000 as tradename.
  - Hence, British Telecom was identified differently by the CAB and the TLSO, but it was assumed the use of the registration number 1800000 refers to the same entity. The conformance attestation were therefore linked to the British Telecom TE individual that resulted from the processing of the UK TL by the program *TL2RDF_UK_EvSPs_v301.xsl*.

- Regarding CertSIGN:
  - CertSIGN was identified by the CAB (LSTI, in their attestation letter) as 'CertSign, AFI Tech Park 1, Bulevardul Tudor Vladimirescu 29, Bucharest, registered in Romania under number J40/484/2006.
  - As the Romanian TL was not processed, it did not receive a TE identifier or an EvSP attestation.
  - The conformity attestation were therefore linked to the entity `http://www.marcsel.eu/onto/te/CertSIGN-SA`, established on the basis of the CAB's attestation letter.

- Regarding Dhimyotis:
  - Dhimyotis was identified by the CAB (LSTI, in their attestation letter) as 'DHIMYOTIS, 20, allée de la Râperie 59650 Villeneuve d'Ascq FRANCE, 20, allée de la Râperie 59650 Villeneuve d'Ascq -FRANCE, without registration information.
  - As the French TL was not processed, it did not receive a TE identifier or an EvSP attestation.
  - The conformity attestation were therefore linked to the entity `http://www.marcsel.eu/onto/te/Dhimyotis`, established on the basis of the CAB's attestation letter.

- Regarding E-Tugra:
  - E-Tugra was identified by the CAB (LSTI, in their attestation letter) as 'E-Tugra Headquarter: 3 Ceyhun Atuf Kansu Cad. Gözde Plaza 130/5806520, Ankara, TURKEY', registered under number 53151.
  - As Turkey is not a member of the European Union, there was no Turkish TL in the European LOTL that could be processed. As a consequence, it did not receive a TE identifier or an EvSP attestation.

  - The conformity attestation were therefore linked to the entity `http://www.marcsel.eu/onto/te/E-Tugra`, established on the basis of the CAB's attestation letter.

- Regarding Zetes:

  - Zetes was identified by the CAB (LSTI, in their attestation letter) as 'ZETES Headquarter: 3 rue de Strasbourg Haren 1130 Bruxelles Belgium' with company registration BE0408425626.
  - Zetes was identified by Belgian TLSO (in https://tsl.belgium.be/tsl-be.xml) by its address and its VAT number VATBE-0408425626. This information was used to allocate the TE identity attestation (te:identifiedBy http://www.marcsel.eu/onto/te/ID-Zetes-SA-NV) to the individual `http://www.marcsel.eu/onto/te/Zetes-SA-NV`.
  - The conformity attestation were therefore linked to the entity `http://www.marcsel.eu/onto/te/Zetes-SA-NV` that resulted from the processing of the Belgian TL by the program *TL2RDF_BE_EvSPs_v301.xsl.*

The file *PDF2RDF_FR_LSTI_EvSPs_v301.rdf* was integrated into the database load file as described in Section 12.16.

12.9 Attestations based on company data

12.9.1 Mapping

12.9.1.1 Available data

A range of data sources for company information were considered for use. An analysis of these sources is provided in Appendix I. It was concluded that the company data from the Global Legal Entities Identification Foundation (GLEIF[53]) that is included in FactForge[54] offers the most suitable choice for the implementation.

12.9.1.2 Used mapping

Since the GLEIF data that is accessible through FactForge is not available in the format of the $\mathcal{TE}$ data model, a transformation is required to map the $\mathcal{TE}$ data model onto the ontologies used in the FactForge GLEIF data. This was done in the following way.

- For the $\mathcal{TE}$ data model, the description from Chapter 7 was used.

[53] An introduction to the GLEIF and its ontologies is provided in Appendix D.2.4
[54] An introduction to FactForge is provided in Appendix I.4

- For the FactForge GLEIF data, the entities referred to by LEIs, and LEIs themselves, are described in the FIBO ontology (see Appendix I.4.2.1) both in natural language and in OWL.

An analysis of the use of the FIBO ontologies in FactForge's GLEIF data is given in Appendix I.4.2. On this basis it was concluded that the following mapping can be made.

- Functional Service Providers/Consumer individuals that are legal persons can be created on the basis of the entities included as legal persons in the GLEIF data.
- The value obtained from the *LegalEntityIdentifier* in the GLEIF data can be used to identify these individuals.

The implementation currently limits its use of FactForge GLEIF data to these two data elements. How to make further use of data published according to the FIBO ontologies is left for future research.

12.9.2 FactForge as data source

12.9.2.1 Application of selection criteria

The company data from the Global Legal Entities Identification Foundation (GLEIF) that is included in FactForge meet the selection criteria, as shown in Table 12.5. Appendix I.3.1 provides additional information on the rationale for selection of the GLEIF data in FactForge for this implementation.

12.9.2.2 Creation of the data source

An individual of the class *te:DataSource* was created for company data based on the FactForge GLEIF data. Information can be retrieved from FactForge using its own upper-level ontology PROTON, or using the ontologies of the included data sets. The latter approach was chosen because it avoids an intermediary mapping ($\mathcal{TE}$ data model $\longleftrightarrow$ PROTON $\longleftrightarrow$ FIBO).

FactForge makes the LEI data available in RDF format, structured according to the Financial Industry Business Ontology (FIBO[56]). According to the FactForge website[57], the FIBO Foundations[58] and the FIBO Business Entities[59] ontologies are included in FactForge. The data source was created in two steps.

- In the first step a selection of the FactForge data was downloaded.

[56] described in appendix D.2.3
[57] `http://factforge.net/`, last accessed 25/1/2021
[58] version 14-11-30, November 2014
[59] version 15-02-23, February 2015

Selection criteria	**Description**	**Comment**
Authoritative source	LEI data is provided by LEI issuers (Local Operating Units, refer to Appendix D.2.4.3) governed by the GLEIF (refer to Appendix D.2.4.1)	This includes the 'Challenge LEI data' mechanism[55] to correct errors in LEI data
Transparency	Available at FactForge's public SPARQL endpoint: `http://factforge.net/sparql`	Data is available as an RDF graph
Description of meaning available	Entities referred to by LEIs, and LEIs themselves are described in the GLEIF (refer to Appendix D.2.4.3) and FIBO (refer to Appendix I.4.2.1) ontologies both in natural language and in OWL	
Machine readable	LEI data is published in RDF/XML format	
Mapping possibility	Mapping is possible via XSLT	
Respect for GDPR [101]	There is no personal information in LEI and related FactForge data	

Table 12.5: Selection criteria for data sources applied to LEI data

  - The SPARQL query described in Listing 12.1 selects the following data.
    - The variable *?name* selects the legal entity's name.
    - The variable *?identifier* selects its LEI.
  - The query response was saved in the local file *FFLEI_20210102.xml*.

- In the second step the file *FF-DataSource-v301.rdf* was created containing an OWL individual of the class *te:DataSource*. This refers to the downloaded data and indicates the FactForge GLEIF data as its original source. This file combines $\mathcal{TE}$ data model predicates and provenance assertions.

The RDF file was integrated into the database load file as described in Section 12.16.

Listing 12.1: FactForge query to select company names and LEIs

```
# http://factforge.net/sparql
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX fibo-be-le-lp: <http://www.omg.org/spec/EDMC-FIBO/BE/LegalEntities/LegalPersons/>
PREFIX fibo-fnd: <http://www.omg.org/spec/EDMC-FIBO/
FND/Foundations/>
PREFIX fibo-fnd-aap-agt: <http://www.omg.org/spec/
EDMC-FIBO/FND/AgentsAndPeople/Agents/>

SELECT ?name ?identifier
WHERE {?indiv rdf:type fibo-be-le-lp:LegalEntity;
                       fibo-fnd-aap-agt:isIdentifiedBy ?identifier ;
              fibo-fnd-aap-agt:hasName ?name. }  limit 100000
```

12.9.3 Creation of Functional Service Providers/Consumers

The program FFLEI2RDF_v301.xsl was run on the downloaded file. The transformation involves the following steps:

- creation of identifiers for individuals, identity attestation, and for FuSP and FuSC role attestation (because it is assumed a legal person can at least act in both roles),
- creation of attestations,
- creation of legal person individuals, including the allocation of identity and role attestations, and enriched with provenance.

The resulting file *FFLEI2RDF_v301.extract.rdf* was integrated into the database load file as described in Section 12.16.

12.10 Endorser

12.10.1 Selection of alternatives

The role of endorser is described in Section 6.5.1 as a participant that publicly expresses approval of a specific rulebook. The endorsement attestation is specified in Section 7.8. The role of endorser can be fulfilled by a government body, or another entity such as an industry or end-user association. Prior to the publication of such an endorsement, the legal consequences thereof would need to be analysed. Such details are outside of the scope of this thesis.

12.11 Enforcer

12.11.1 Selection of alternatives

The role of enforcer is described in Section 6.5.1 and the enforcement attestation is specified in Section 7.9. Competence and authority in matters of law enforcement are complex. The eIDAS Regulation [103] was identified as relevant legislation for trust and trustworthiness. Similar legislation exists for non-EU countries. A description of the legal perspective is provided in Section 2.2.3.

As the eIDAS regulation is a European legal instrument, one could argue that the European Court of Justice takes the role of enforcer on the basis of the self-provided role description on the Court's website[60]. Furthermore data is available from open data sources, e.g. the European Data Portal publishes information on the judicial systems in EU Member States[61]. However, for participants that originate outside the EU, this would most likely not be suitable. Determining a more appropriate authority (or authorities) to fulfil the role of enforcer for the rulebook proposed here is a legal matter more than an information security matter.

We suppose here that it is possible to identify the legally competent authority (or authorities) regarding the participants and their attributes. As this is a legal matter, it is outside the scope of this thesis.

12.12 Data sources for natural persons

A range of public data sources were considered for use, and those adopted are listed below. An analysis of these sources is provided in Appendix J. Authentic sources (such as national identity registers) are highly relevant, but use of such data is restricted under legislation such as GDPR [101]. It was concluded that the following were relevant candidates for this implementation.

[60] `https://curia.europa.eu/`

[61] `https://www.europeandataportal.eu/data/datasets/`, see information on judicial systems in Member States ordinary courts

- An aggregated FOAF file from Elsevier's Mendeley Data Search[62].
- A sample certificate of a natural person (the author of the thesis), produced on behalf of a national identity register.

For each candidate data source, the possible data items that could be mapped onto predicates were identified, and the selection criteria specified in Section 12.2.1 were applied. Where this application led to the conclusion that the use of the data source was justified, a download and transformation mechanism was established. This is described for FOAF data and national identity data below.

12.13 Natural Persons based on FOAF data

12.13.1 Mapping

Natural persons can act in the $\mathcal{TE}$ framework as Functional Service Consumers or Providers (through the use of software agents). These roles were described in Section 6.5.3. An analysis of the available data from FOAF information providers led to the conclusion that a FOAF natural person corresponds sufficiently to a $\mathcal{TE}$ framework natural person for this implementation. The rationale for this conclusion is as follows.

The FOAF specification is defined as a dictionary of named properties and classes using W3C's RDF semantics and syntax. Since the FOAF data model is different from the $\mathcal{TE}$ data model, a transformation is required. Therefore a mapping must be defined.

- For the $\mathcal{TE}$ data model, the description from Chapter 7 was used.
- For the information published in FOAF files, the human-readable FOAF Vocabulary Specification [37] and the machine-readable RDF version[63] were used.
  - The FOAF specification describes a broad set of person-related attributes including name, homepage, work location, email address, and a hash of an email address.
  - The FOAF specification can also contain relationship information. This means that a person's FOAF file can contain records with the *foaf:knows* attribute, which refers to other persons. By mentioning other people (via *foaf:knows* or other relationships) and by providing an *rdfs:seeAlso* link to their FOAF file, FOAF indexing tools can build FOAF aggregators without the need for a centrally managed directory of FOAF files.

    This relationship information is not used by the $\mathcal{TE}$ predicates.

[62] `https://www.elsevier.com/solutions/mendeley-data-platform`
[63] `http://xmlns.com/foaf/spec/index.rdf`

A comparison of the FOAF and $\mathcal{TE}$ data model descriptions led to the conclusion that the following mapping can be used.

- The *foaf:Person* class[64] represents people and corresponds to the *te:NaturalPerson* class. Such people can be attested in roles, e.g. as Functional Service Consumer or Provider.
- There are two properties related to an email mailbox.
  - The *foaf:mbox* property is a relationship between the owner of a mailbox and a mailbox. A mailbox is an Internet mailbox associated with exactly one owner. This is a 'static inverse functional property', in that there is (at any point in time) at most one individual that has a particular value for *foaf:mbox*. Mailboxes are typically identified using the *mailto:* URI scheme [150]. FOAF sees mbox as an indirect way of identifying its owner, which works even if the mailbox is out of service. Furthermore, a person can have multiple mbox properties.

    The *foaf:mbox* property can be used to create a unique $\mathcal{TE}$ identifier of a person.
  - The *foaf:mbox_sha1sum* property is a textual representation of the result of applying the SHA-1 [257] hash function to a 'mailto:' identifier for an Internet mailbox with which a person has an mbox relationship.

    The *foaf:mbox_sha1sum* property can also be used to create a unique $\mathcal{TE}$ identifier of a person, and is more privacy-friendly.
- The *foaf:familyName*, *foaf:givenName*, *foaf:lastName* and *foaf:firstName* properties describe names of a person.

  These can be used as identity attributes.
- The following list is a selection of properties which could be used as additional identity attributes.
  - The *foaf:img* property refers to an image.
  - The *foaf:birthday* property describes a birthday.
  - The *foaf:nick* property describes a nickname.
  - The *foaf:openid* property describes an OpenID identifier.
  - The *foaf:phone* property describes a telephone number.
  - The *foaf:publications* property describes publications associated with the person.
  - The *foaf:skypeID* property describes a Skype identifier.

[64] The *foaf:Person* class is a sub-class of *foaf:Agent*, which further includes *foaf:Organization* and *foaf:Group*.

Selection criteria	Description
Authoritative source	FOAF data is self-provided.
Transparency	FOAF data is published in readable format by its owner, aggregated in Academic databases such as Mendeley
Description of meaning available	The FOAF terminology is described in the FOAF specification [37]
Machine readable/human readable	FOAF data is published in machine readable XML Schema Description (XSD) format
Mapping possibility	Data elements can be mapped via XSLT
Respect for GDPR [101]	There is personal information in FOAF data but it is self-disclosed by its owner so it seems reasonable to assume consent is present. FOAF data may contain information about other persons known to the publisher, but such information is not used in the thesis.

Table 12.6: Selection criteria for data sources applied to FOAF data

12.13.2 FOAF data as data source

12.13.2.1 Application of selection criteria

FOAF data sources and their data meet the selection criteria defined in Section 12.2.1, as described in Table 12.6. They provide relevant data sources for natural person predicates.

To adhere to requirements IR2 (transparency) and IR7 (data source credibility), the provenance of the information used to bind variable occurrences must be included. As a consequence all use of FOAF data as data source needs to refer to the original source. $\mathcal{TE}$ data sources that include a link to the original FOAF source were created for this purpose. For the implementation, two data sources were established on the basis of the Mendeley database. Each data source corresponds to one FOAF file.

12.13.2.2 Use and transformation

The approach described in Section 12.5.2.2 was applied to the FOAF data. The FOAF data set[65] [272] that was used as a data source was obtained from Elsevier's Mendeley Data service. It is described by Petrovic and Fujita [273]. The dataset contains FOAF descriptions of 84802 people, and 107485 known relationships. These were extracted from the Advogato social networking site[66].

[65] `https://data.mendeley.com/datasets/zp23s23xpb/1`

[66] `http://www.advogato.org/`, with `http://www.advogato.org/person/connolly/foaf.rdf\#me` as the initial URL

The Mendeley dataset consists of a compressed file. Its decompression results in a series of individual FOAF files. Two XSL programs[67] were developed to create $\mathcal{TE}$ model data sources on the basis of such FOAF files. The programs combines $\mathcal{TE}$ data model predicates and provenance assertions. The provenance assertions describe the following:

- the activity (*prov:Activity*) that created the data source, including the time when the activity was performed (*prov:startedAtTime* and *prov:endedAtTime*);
- the original source from where the data source was derived (*prov:wasDerivedFrom*), i.e. the URI of the Mendeley data set;
- the agent to which the creation of the data source can be attributed, for which a reference to *http://www.marcsel.eu/ti* is used, referring to the $\mathcal{TE}$ framework's data integration software.

The XSL program involves the following two steps.

- The first step is the creation of the Activity individual that generates the data source. This involves the creation of a resource with a hardcoded name based on the XSL program and its execution date (*http://www.marcsel.eu/onto/te/xsl/FOAF_01_DataSource_v301.xsl.2021-01-07*), its casting into the type of *prov:Activity* and the addition of *prov:startedAtTime* and *prov:endedAtTime*.
- The second step is the creation of the DataSource individual. This involves the creation of a resource with a hardcoded name based on the URI from where the FOAF file was originally obtained by the aggregator that published it on the Mendeley data service, its casting into type *te:DataSource*, the addition of the Mendeley URI (as *prov:wasDerivedFrom*) and the addition of further provenance data.

The output of the transformations was integrated into the database load file as described in Section 12.16.

12.13.3 NPs based on FOAF data

Two XSL programs[68] were used to create natural persons. The programs combine $\mathcal{TE}$ data model predicates and provenance assertions in a similar way to the corresponding data source program. Each program used a different FOAF file as its input. The transformation involves the following steps:

[67] *FOAF_01_DataSource_v301.xsl* and *FOAF_02_DataSource_v301.xsl*
[68] called *FOAF_01_NP_v301.xsl* and *FOAF_02_NP_v301.xsl*

- creation of identifiers for identity and role attestations and for the natural person, including provenance data,
- creation of identity and role attestations,
- creation of the NaturalPerson individuals, as a resource with its name based on *foaf-name*, the casting into type of *te:NaturalPerson*, and the inclusion of identity and role attestations and provenance data.

For privacy reasons, only those persons whose FOAF file included the *foaf:mbox_sha1sum* attribute were selected from the outputfile for inclusion in the database load file. These records were integrated into the database load file as described in Section 12.16. Figure 12.2 shows a FOAF-based Natural Person and its properties in GraphDB's explorer.

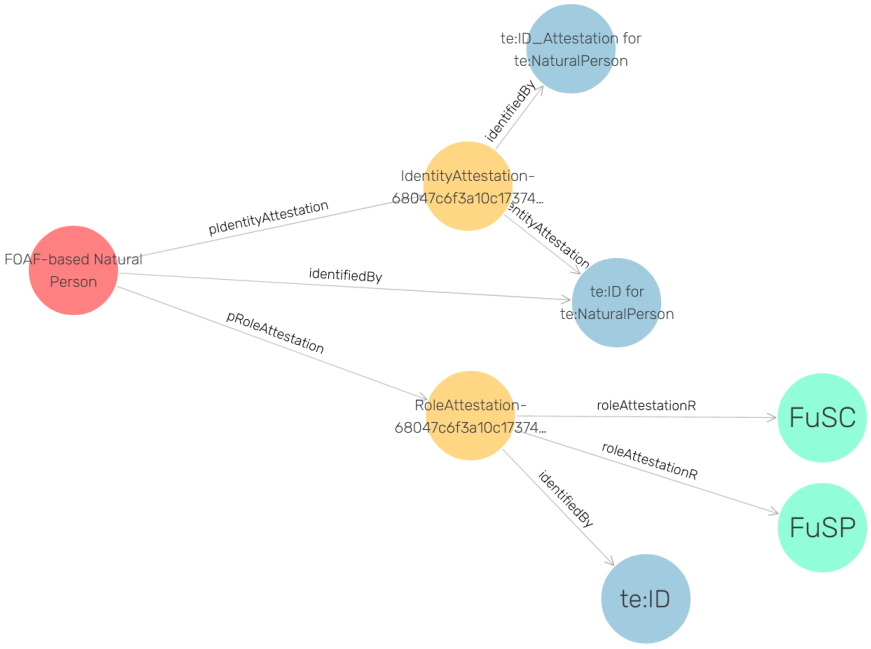

Figure 12.2: FOAF-based Natural Person and its properties

12.14 NPs based on national identity data

12.14.1 Mapping

Natural persons can act in the $\mathcal{TE}$ framework as Functional Service Consumers or Providers. These roles were described in Section 6.5.3. The analysis of the available data from national identity data sources described in Appendix J led to the conclusion that a natural person as

Selection criteria	Description
Authoritative source	National identity data is provided by a national competent authority
Transparency	National identity data is distributed in certificate files, which are used to verify e.g. the authenticity of an email or an electronic document, or an on-line authentication ticket
Description of meaning available	The format used by these certificates is described in the X.509 version 3 specification [63]
Machine readable/human readable	National identity data is published in PEM or DER encoding which is easily decoded
Mapping possibility	Data elements can be mapped manually
Respect for GDPR [101]	There is personal information in national identity data, hence respect for GDPR [101] has to be evaluated on a case-by-case basis

Table 12.7: Selection criteria for data sources applied to national identity data

described in such a source corresponds sufficiently to a $\mathcal{TE}$ framework natural person for our purposes. However, as all national identity data sources are different, the mapping must be tailor-made. For the implementation, this was done for Belgium only.

12.14.2 NID as data source

12.14.2.1 Application of selection criteria

National identity data is not generally available. However, in a number of countries the government distributes X.509 certificates for authentication and signature. In countries such as Belgium and Spain, these certificates contain citizen identity data which is based on the authentic source, the national identity register. There is no general access to the national identity register; however, the certificates are used in the public domain because they are included in the electronic identity cards, and are required when validating an on-line authentication request or a signature.

National identity data provides relevant data sources for natural person predicates. Such data partially meets the selection criteria defined in Section 12.2.1 as described in Table 12.7. It was decided to include data for a single natural person (the author of the thesis) to demonstrate the possibilities of this data.

12.14.2.2 Use and transformation

For the implementation of a natural person based on national identity data, the following components were created.

- An individual that represents the Belgian National Register of Natural persons (NRN) as authentic source of identity information.
- A data source that represents an X.509 certificate based on this authentic source.

The individual that represents the NRN as authentic source of identity information was created manually in the file *BE-AS-NRN-v301.rdf*. The NRN is part of the Belgian Federal Public Service Home Affairs.

The NRN individual asserts:

- that it was derived from the law[69] that established the organisation,
- links to identity and role attestations, based on the electronic publication, by the Belgian Ministry of Justice in the official State Gazette, of the law that established the organisation, and
- that it was attributed to this same electronic publication.

The data source file *Certipost-CitizenCA-cert-01-DataSource-v301.rdf* was created manually. The data source asserts:

- that it was derived from the certificate downloaded from an eID card,
- that the certificate was made available[70], and
- that it was attributed to Certipost.

Both files were integrated into the database load file as described in Section 12.16.

12.14.3 NPs based on national identity data

The authentication certificate file of a Belgian citizen was extracted from an identity card and saved[71]. This certificate file contains the following information:

[69] http://www.ejustice.just.fgov.be/eli/wet/1983/08/08/1984021127/justel

[70] at `http://www.marcsel.eu/onto/te/crt/Certipost-CitizenCA-01-NP-v301.crt`

[71] The encoded certificate is available at `http://www.marcsel.eu/onto/te/crt/Certipost-CitizenCA-01-NP-v301.crt`. The certificate can be decoded into human readable format using the OpenSSL tool from `https://www.openssl.org/` or an on-line decoder such as e.g. `https://redkestrel.co.uk/products/decoder/`.

- Regarding the certificate's subject: 'C=BE, CN=Marc Sel (Authentication), SN=Sel, GN=Marc Louis, serialNumber=**********' (the serial number is equal to the national identity register number of the citizen and has been removed for privacy reasons),
- Regarding the certificate's issuer: 'C=BE, CN=Citizen CA, serialNumber=201403',
- Information on
  - validity period and cryptographic algorithms and key-lengths used,
  - 'Authority Information Access' information about the issuer,
  - Certificate Policy: OID and url of the CPS,
  - CRL distribution point.

The information in the certificate was used to manually create two pieces of information.

- The *Certipost-CitizenCA-01-NP-v301.rdf* file, containing:
  - the resource BE-Marc-Louis-Sel[72] as a *te:NaturalPerson*,
  - with an identity attestation issued by Certipost[73],
  - derived from the corresponding data source[74].
- A conformance attestation was added to file *DBLN.owl*. The attestation was given the name *Demo-Conformance-001*[75] because it demonstrates how conformity to a level of identity proofing can be incorporated in the $\mathcal{TE}$ framework on the basis of existing information.

This file was integrated into the database load file as described in Section 12.16.

12.15 Self-attestations

It can reasonably be expected that self-attestations are available when entities provide information about themselves in a publicly available electronic way. In the context of the thesis it was decided to use existing data rather than to request self-attestations. For natural persons, the FOAF data that was discussed in Section 12.13 provided a relevant example. For organisations, their websites were a relevant source of information. File *DBLS.owl* provides examples

[72] in full `http://www.marcsel.eu/onto/te/BE-Marc-Louis-Sel-212676479325589833081964577000153656695`, using the certificate's serial number as a suffix for the resource name

[73] in full `http://www.marcsel.eu/onto/te/Certipost-NV-SA`

[74] `http://www.marcsel.eu/onto/te/rdf/Certipost-CitizenCA-cert-DataSource-v301.rdf`

[75] In full: `http://www.marcsel.eu/onto/te/Demo-Conformance-001`

of self-attestations of organisations (Certipost, Zetes and SMETS1 PKI-Service from Secure Meters Limited) based on their website. This file was integrated into the database load file as described in Section 12.16.

12.16 Data integration

12.16.1 Overview

The outputs of all transformations were included in a single XML/RDF file called *DBL.owl*. This integrated file is referred to as the database load file. The construction of the database load file is described in Appendix L.

12.16.2 Loading

The database load file can be loaded into any tool supporting the RDF/XML format. The file was loaded into an instance of the Ontotext GraphDB database. The following figures illustrate some selected features of the loaded file.

- Figure 12.3 shows the $\mathcal{TE}$ data model class hierarchy in the explorer of GraphDB.
- Figure 12.4 shows an overview of the $\mathcal{TE}$ data model class relationships in the explorer of GraphDB.
- Figure 12.5 shows a sample participant, the British Telecom evidence service provider as represented in the $\mathcal{TE}$ data model graph.

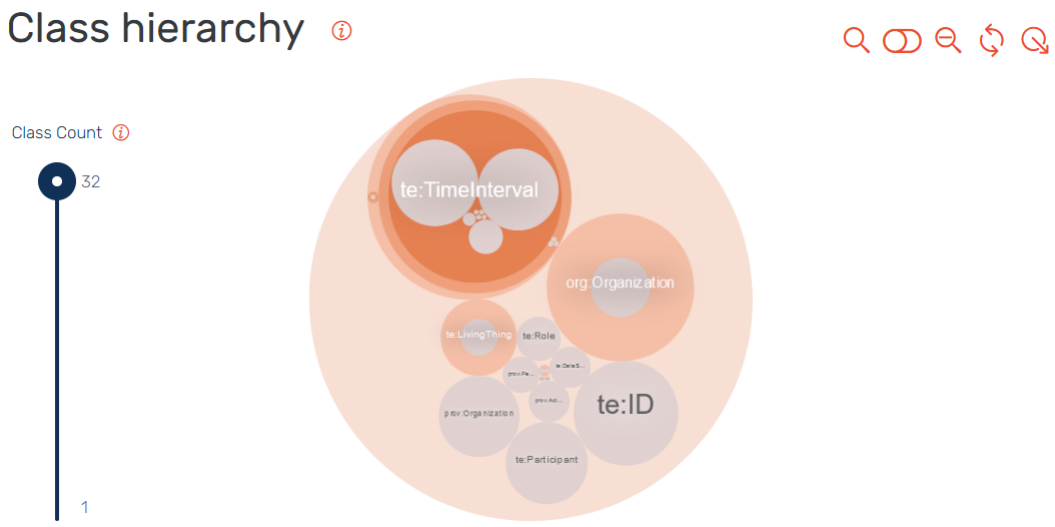

Figure 12.3: The $\mathcal{TE}$ data model class hierarchy

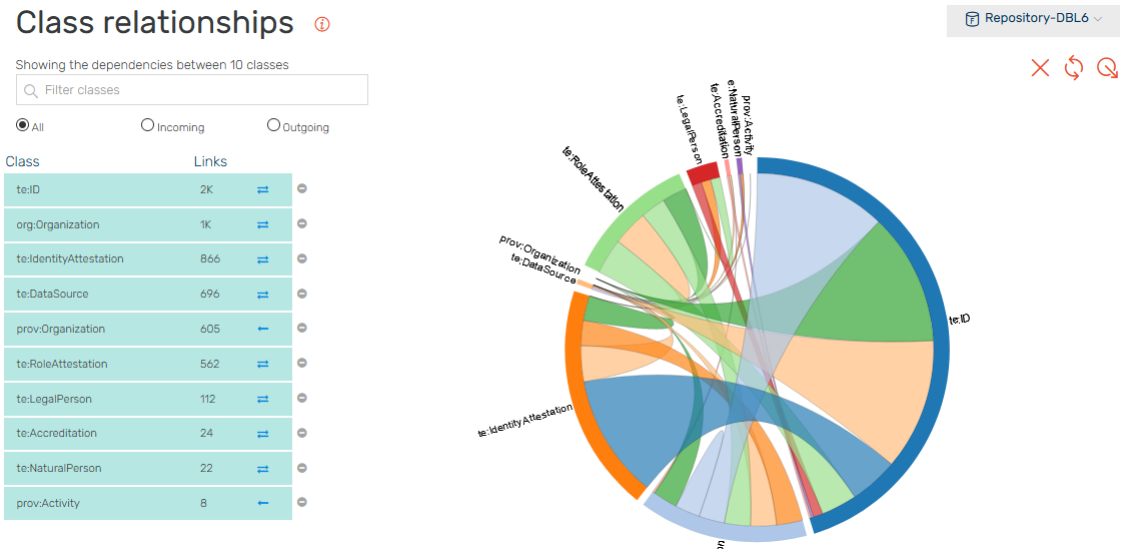

Figure 12.4: Overview of the $\mathcal{TE}$ data model class relationships

Figure 12.5: The British Telecom evidence service provider and related classes as represented in the $\mathcal{TE}$ data model graph

12.17 Summary

This chapter presented the implementation of a mechanism for the import and transformation of instance data for the data model implementation described in Chapter 11. This included the selection of data sources, the download of data and its transformation into the $\mathcal{TE}$ data model format, and the addition of provenance information.

The approaches that were used for selection, download, transformation and integration of data were presented. The technical set-up of the technology used was discussed. This included the creation of an Eclipse project that allows the execution of XSL transformations on the selected data, and the creation of a GraphDB repository. Candidate data sources were identified and described. The creation of individuals, through the use of XSL transformations, was demonstrated. This was done for the following predicates:

- trustworthiness monitors and evidence service providers (on the basis of public trusted lists).
- accreditation bodies and conformity assessment bodies (on the basis of public accreditation data);
- authentic sources and norms (based on public company data);
- legal persons (based on public company data);
- natural persons (based on public data).

The creation of endorser and enforcer individuals was discussed but no such individuals were created. How the transformed data was integrated and loaded into a graph database was described.

This implementation contributes to the validation of the proposed framework by creating a database that contains information corresponding to the 'real world' of the selected data sources and participants. This information is used in Chapters 13 and 14.

Chapter 13

Implementation of a rulebook

An implementation of a specific rulebook, i.e. a set of constraints that reflect a particular context for reasoning about trustworthiness, is presented. The implemented rulebook is β_{AP}, described in Chapter 8, the content of which was inspired by the European legislation for trust services.

13.1 Introduction

This chapter presents a partial implementation of a specific rulebook. The concept of a rulebook was introduced in Chapter 8 as a set of constraints that reflect a particular context for reasoning about trustworthiness. The example rulebook β_{AP} was specified in Sections 8.9 – 8.13; it was inspired by the European legislation on trust services itself described in Section 2.2.3.

In this chapter we describe a partial implementation of this example rulebook. The implementation of the data model described in Chapter 11, and of the data import and transformation mechanism described in Chapter 12, are based on a graph database. As a consequence, the rulebook implementation makes use of the features of a graph database and consists of:

- constraints imposed by properties of the data model, and
- SPARQL queries.

The implementation of the data model and of the data import and transformation mechanism is complemented by an implementation of a subset of the rules defined in Chapter 8. The rules derived from requirements IR2 (transparency) and IR3 (linked and unique identity) were implemented and a subset of the rules derived from requirement IR4 (competently acting in role) were implemented. Whilst the remaining rules (namely the other rules derived from requirement IR4 and those derived from IR5) have not been implemented, it should be a relatively straightforward task to implement them following the same approach.

The remainder of this chapter is structured as follows.

- Section 13.2 describes the general approach to implementing the rulebook.
- Section 13.3 describes the technical set-up.
- Section 13.4 addresses the implementation of rules derived from requirement IR2 *Transparency*.
- Section 13.5 addresses the rules derived from requirement IR3 *Linked and unique identity*.
- Section 13.6 addresses a selection of the rules derived from requirement IR4 *Competently acting in role*.
- Section 13.7 provides a summary.

13.2 Approach

The rulebook specified in Chapter 8 is structured according to the integrated set of requirements, given in Section 5.5, as follows.

- Requirement IR1 (semantic definition of trustworthiness, described in Section 5.5.1) was addressed by formulating the rules in FOL using a formal taxonomy over data points that have a truth-functional interpretation.
- Requirement IR6 (policy choices, described in Section 5.5.6) was addressed by structuring rules into two sets, containing mandatory and discretionary rules.
- Requirement IR7 (credible data, described in Section 5.5.7) was addressed by using data sources as specified in Section 12.2.

The rules derived from requirements IR2, IR3 and partially from IR4, were implemented in the following way.

- As described below, each rule was implemented either in the form of:
  - constraints, imposed by properties of the $\mathcal{TE}$ data model, or
  - a SPARQL query together with an expected response to this query.
- A rulebook data file was created which includes all the queries corresponding to rules of the rulebook. The RIPEMD-160 and SHA 256 digests of the file were calculated using CrypTool[1].

[1] `https://www.cryptool.org/en/`

- A rulebook individual including provenance information was manually created and integrated into the database load file, as described in Section 12.16.

13.3 Set-up

13.3.1 Inferencing

The implementation makes use of Protégé as a data modeller and GraphDB as a database. Both were introduced in Section 10.3. Because their inferencing capabilities influence the implementation it is important to understand these capabilities.

- The SPARQL support in Protégé 5.5 has the limitation that it does not allow information created through inference to be queried. It is possible to partially overcome this limitation by using the plug-in *Snap SPARQL*. Its support for inferences to be queried is described by Horridge and Musen [152]. However, while this plug-in allows inferences to be queried, it does not support the SPARQL *ASK* statement that provides a means of obtaining a yes/no answer to a query, and is helpful in the implementation.
- Fortunately, Ontotext's GraphDB does support SPARQL queries on information created through inference.

As a consequence, prototyping of queries was done in Protégé, but the development was done in Ontotext's GraphDB.

13.3.2 Using interactive queries

To develop and execute the SPARQL queries that implement the rules, the GraphDB Workbench was used. Once a GraphDB database is started, the GraphDB Workbench is accessible through a browser (at `http://localhost:7200/`) and the database load file can be imported (from `http://www.marcsel.eu/onto/te/DBL.owl`). To have inferred data accessible in queries, the button 'Include Inferred data' needs to be in the position 'on'.

13.3.3 Rulebook

A copy of the rulebook is available at `http://www.marcsel.eu/onto/te/RuleBook-001.txt`.

Listing 13.1: IR2-M01

```
# IR2-M01
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
ASK {?a rdf:type te:RuleBook . }
```

Listing 13.2: Listing all rulebooks

```
# Listing all rulebooks
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
# Listing all rulebooks
select * where {?RulebookIndividual rdf:type te:RuleBook . }
```

13.4 IR2 Transparency

13.4.1 Mandatory rules

The mandatory rules are specified in Tables 8.1 and 8.2. The rules contained in Table 8.1 (the rulebook-related rules) were implemented in the following way.

- Rule $\beta_{IR2\text{-}M01}$ (a trustworthy ecosystem must have at least one rulebook) was implemented by the ASK query described in Listing 13.1, the expected response to which is 'YES'. Existing rulebooks can be listed as described in Listing 13.2, the expected response to which is a list of candidate rulebooks.

- Rule $\beta_{IR2\text{-}M02}$ (every rulebook must be uniquely identified) was implemented by using the object property *te:doesIdentify* as described in Section 11.5. Whether there is an identifier linked through the property *te1:doesIdentify* can be queried as described in Listing 13.3. The expected response is a list of rulebook-identifiers pairs, indicating valid rulebooks. Inspection of the identifier reveals the unique identifier and the provenance data of the rulebook.

Table 8.2 contains $\beta_{IR2\text{-}M10}$ the participant-related rule. This rule (a participant is an actor that has a given name (for a natural person) or an organisation name (for an organisation)) is implemented in the data model implementation, as described in Section 11.7.2. It can be queried as described in Listing 13.4. The expected response is a list of candidate participants. Such participants have a name but not necessary one or more identity attestations. This latter property is verified in IR3-M01.

Listing 13.3: IR2-M02

```
# IR2-M02
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
select * where {
    ?rulebook rdf:type te:RuleBook .
        ?id te:doesIdentify  ?rulebook .
}
```

Listing 13.4: IR2-M10

```
# IR2-M10
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX terms: <http://purl.org/dc/terms/>
select * where {
    ?Participant rdf:type te:Participant .
}
```

13.4.2 Discretionary rules

As rulebook β_{AP} does not contain discretionary rules for IR2, there is nothing to implement. To demonstrate how rules of this type could be implemented, Appendix N describes an implementation of the discretionary rules for IR 2 for the rulebook β_{AE}.

13.5 IR3 Linked and unique identity

13.5.1 Mandatory rules

The single mandatory rule $\beta_{IR3\text{-}M01}$ (a participant is an actor that is uniquely identified) is specified in Table 8.4. The rule was implemented in the same way as IR2-M02, i.e. by using the object property *te:doesIdentify* described in Section 13.4.1. The existence of a identifier can be verified as described in Listing 13.5. The expected response is a list of participant-identifier pairs, indicating valid participants. Inspection of the identifier (e.g. through the GraphDB Workbench) reveals the unique identifier and the provenance data of the participant.

13.5.2 Discretionary rules

The discretionary rules regarding linked and unique identity are specified in Tables 8.23 to 8.28

Listing 13.5: IR3-M01

```
# IR3-M01
select * where {
    ?participant rdf:type te:Participant .
        ?id te:doesIdentify  ?participant .
}
```

Listing 13.6: IR3-D11-AP

```
# IR3-D11-AP
select * where {
        ?Participant rdf:type te:Participant .
    ?Participant te:pIdentityAttestation ?identityAttestation .
    ?identityAttestation prov:wasAttributedTo ?issuerOfIdentityAttestation.
    FILTER (?Participant = ?issuerOfIdentityAttestation ) .
}
```

Listing 13.7: IR3-D11b-AP

```
# IR3-D11b-AP
ask { te:Zetes-SA-NV te:pIdentityAttestation ?identityAttestation .
    ?identityAttestation prov:wasAttributedTo ?issuerOfIdentityAttestation.
}
```

Table 8.23 specifies the single rule regarding self-attestation, $\beta_{IR3\text{-}D11\text{-}AP}$ (a participant's identity must be self-attested). This was implemented as described in Listing 13.6. The expected response is the list of participants that have at least one identity attestation that is self-attested.

The related query that asks whether a particular participant is linked to a self-attested identity attestation was implemented as described in Listing 13.7. The company Zetes was used as an example. The expected response is yes. In the case of Zetes a yes answer is obtained because Zetes is a participant for which a self-attestation is present in the database load file, as described in Section 12.15.

The related query that identifies participants that lack self-attested identity attestation was implemented as described in Listing 13.8. The expected response is the list of participants that lack self-attested identity attestations.

Listing 13.8: IR3-D11c-AP

```
# IR3-D11c-AP
select * where {
        ?Participant rdf:type te:Participant .
    MINUS {?Participant te:pIdentityAttestation ? identityAttestation .
                ?identityAttestation prov:wasAttributedTo ?issuerOfIdentityAttestation
        FILTER (?Participant = ?issuerOfIdentityAttestation ) }.
}
```

Rules regarding attestations other than self-attestations are specified in Tables 8.24 through 8.28. The rules contained in Table 8.24 were implemented in the following way.

Rule $\beta_{IR3\text{-}D21\text{-}AP}$ (for the selected participant there must at least one identity attestation that is not self-attested) was implemented as described in Listing 13.9. The expected response is a table that contains a list of participants that have at least one identity attestation that is not

Listing 13.9: IR3-D21-AP

```
# IR3-D21-AP
select * where {
        ?Participant rdf:type te:Participant .
    ?Participant te:pIdentityAttestation ?identityAttestation .
    ?identityAttestation prov:wasAttributedTo ?issuerOfIdentityAttestation.
    FILTER (?Participant != ?issuerOfIdentityAttestation ) .
}
```

Listing 13.10: IR3-D22-AP

```
# IR3-D22-AP
select * where {
        ?Participant rdf:type te:Participant .
        ?Participant te:pIdentityAttestation ?identityAttestation .
    ?identityAttestation prov:wasAttributedTo ?issuerOfIdentityAttestation.
    ?issuerOfIdentityAttestation te:pRoleAttestation ?RoleAttestation .
    ?RoleAttestation te:roleAttestationR te:EvSP.
}
```

self-attested, and the trustor must verify whether the selected participant is included in the list[2].

Rule $\beta_{IR3\text{-}D22\text{-}AP}$ (the identity of the selected participant must be attested to by at least one evidence service provider) was implemented as described in Listing 13.10. The expected response is a table that contains a list of participants that have at least one identity attestation that is attested to by an evidence service provider. The trustor must verify whether the selected participant is included in the list. An alternative implementation is possible by using the name of the selected participant.

Rule $\beta_{IR3\text{-}D23\text{-}AP}$ (the identity of the selected participant must be attested to by at least one evidence service provider attested in its role by a trustworthiness monitor) was implemented as described in Listing 13.11. The expected response is a table that contains a list of participants that meet the constraint, and the trustor must verify whether the selected participant is included in the list. An alternative implementation is possible by using the name of the selected participant. In addition to the name, the resulting table contains the following attributes:

- the participant's identity attestation (variable ?P1IdentityAttestation),
- the issuer of the identity attestation (variable ?P2issuerOfP1IdentityAttestation),
- the role of this issuer (participant P2 must be an EvSP),
- the identity of issuer of this role attestation (variable ?P3issuerOfEvSProle) and its role (participant P3 must be a TwsMo),

[2] An alternative implementation is possible by using the name of the selected participant. How to use the name of the selected participant is demonstrated in Listing 13.7.

Listing 13.11: IR3-D23-AP

```
# IR3-D23-AP
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
# all participants'_identity_must_be_attested_by_an_evidence_service_provider_attested_in_its_role_by_a_
    trustworthiness_monitor
?Participant1_rdf:type_te:Participant_.
?Participant1_te:pIdentityAttestation_?P1identityAttestation_.
?P1identityAttestation_prov:wasAttributedTo_?P2issuerOfP1IdentityAttestation.
?P2issuerOfP1IdentityAttestation_te:pRoleAttestation_?RoleAttestationOfP2_.
?RoleAttestationOfP2_te:roleAttestationR_te:EvSP_.
#_that_EvSP_corresponds_to_?P2issuerOfP1IdentityAttestation
#__which_must_be_attested_in_its_role_by_a_trustworthiness_monitor
?RoleAttestationOfP2_prov:wasAttributedTo_?P3issuerOfEvSProle_.
?P3issuerOfEvSProle_te:pRoleAttestation_?RoleAttestationOfP3_.
?RoleAttestationOfP3_te:roleAttestationR_te:TwsMo_.
#_display_the_role_that_is_attested_explicitly
?RoleAttestationOfP3_te:roleAttestationR_?Role_.
}
```

- the role of P3 (variable ?Role).

The rules contained in Table 8.25 address requirements regarding the verification of the binding between an applicant and its identity prior enrolment, using ISO/IEC TS 29003:2018 Level 2 and Level 3, respectively.

These rules were implemented in the following way. Rule $\beta_{IR3\text{-}D24\text{-}AP}$ was implemented as described in Listing 13.12. The expected response is a list of participants that meet rule $\beta_{IR3\text{-}D24\text{-}AP}$. Rule $\beta_{IR3\text{-}D25\text{-}AP}$ is implemented by replacing *te:ISO-IEC-TS-29003:2018:LOIP2* by *te:ISO-IEC-TS-29003:2018:LOIP3* in Listing 13.12. The expected response is a list of participants that meet rule $\beta_{IR3\text{-}D25\text{-}AP}$.

Rules relating to identity attestation by legally qualified entities are given in Table 8.26. These rules were implemented in the following way.

Rule $\beta_{IR3\text{-}D31\text{-}AP}$ (the identity of the selected participant must be attested to by at least one evidence service provider who is legally attested in that role) was implemented as described in Listing 13.13. The expected response is a table that contains a list of participants that meet the constraint, and the trustor must verify whether the selected participant is included in the list. An alternative implementation is possible by using the name of the selected participant. The list contains the following elements.

- The participant's name (?Participant1).
- The identity attestation (?P1IdentityAttestation) and the issuer thereof (?P2IssuerOfP1IdentityAttestation).
- The role attestation of this issuer (?RoleAttestationOfP2).

Listing 13.12: IR3-D24-AP

```
# IR3-D24-AP
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
# Step 1 select EvSPs that attest to identity
# ?Participant1 = selected participant
?Participant1 rdf:type te:Participant .
?Participant1 te:pIdentityAttestation ?P1identityAttestation .
?P1identityAttestation prov:wasAttributedTo ?P2issuerOfP1IdentityAttestation.
?P2issuerOfP1IdentityAttestation te:pRoleAttestation ?RoleAttestationOfP2 .
?RoleAttestationOfP2 te:roleAttestationR te:EvSP .
# EvSP = ?P2issuerOfP1IdentityAttestation
# which must be attested in its role by a trustworthiness monitor
# TwsMo = ?P3issuerOfEvSProle
?RoleAttestationOfP2 prov:wasAttributedTo ?P3issuerOfEvSProle .
?P3issuerOfEvSProle te:pRoleAttestation ?RoleAttestationOfP3 .
?RoleAttestationOfP3 te:roleAttestationR te:TwsMo .
# display the role that is attested explicitly
?RoleAttestationOfP3 te:roleAttestationR ?Role .

# Step 2 select EvSP that conforms to ISO-IEC-TS-29003 according to TwsMo
# Select conformance attestations of P1
?P2issuerOfP1IdentityAttestation te:pConformance ?IdentityAttestationConformance .
# Select only those conformance attestations from the selected TwsMo
?IdentityAttestationConformance prov:wasAttributedTo ?P3issuerOfEvSProle .
# Select only those conformity attestations that match LOIP2
?IdentityAttestationConformance te:conformanceN te:ISO-IEC-TS-29003:2018:LOIP2 .
# Display the norm for information purpose
?IdentityAttestationConformance te:conformanceN ?IdentityNorm .
}
```

- The legal qualification (?LegalRoleQualification) and the legal document (?LegalNorm) on which the role attestation is based.

Rule $\beta_{IR3\text{-}D32\text{-}AP}$ which states:

- that the identity of the selected participant must be attested to by at least one evidence service provider attested to its role by a trustworthiness monitor; and
- that the evidence service provider and the trustworthiness monitor must be legally attested in their respective roles,

Listing 13.13: IR3-D31-AP

```
# IR3-D31-AP
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
# The participant identity must be attested by an EvSP
?Participant1 rdf:type te:Participant .
?Participant1 te:pIdentityAttestation ?P1identityAttestation .
?P1identityAttestation prov:wasAttributedTo ?P2issuerOfP1IdentityAttestation.
?P2issuerOfP1IdentityAttestation te:pRoleAttestation ?RoleAttestationOfP2 .
?RoleAttestationOfP2 te:roleAttestationR te:EvSP .
# Alternative form to catch all roles: ?RoleAttestationOfP2 te:roleAttestationR ?RoleOfP2 .

# The EvSP corresponds to ?P2issuerOfP1IdentityAttestation
#  which must be legally attested in its role
?RoleAttestationOfP2 te:raLegalQualification ?LegalRoleQualification .
# Display the legal norm for information purpose
?LegalRoleQualification te:legalQualificationN ?LegalNorm.
}
```

Listing 13.14: IR3-D32-AP

```
# IR3-D32-AP
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
?Participant1 rdf:type te:Participant .
?Participant1 te:pIdentityAttestation ?P1identityAttestation .
?P1identityAttestation prov:wasAttributedTo ?P2issuerOfP1IdentityAttestation.
?P2issuerOfP1IdentityAttestation te:pRoleAttestation ?RoleAttestationOfP2 .
?RoleAttestationOfP2 te:roleAttestationR te:EvSP .
# To display the EvSP's_role_attestation
?RoleAttestationOfP2_te:roleAttestationR_?RoleOfP2_.

#_EvSP_must_be_attested_by_TwsMo
#__EvSP_corresponds_to_?P2issuerOfP1IdentityAttestation
#__TwsMo_corresponds_to_?P3issuerOfEvSProle
?RoleAttestationOfP2_prov:wasAttributedTo_?P3issuerOfEvSProle_.
?P3issuerOfEvSProle_te:pRoleAttestation_?RoleAttestationOfP3_.
#?RoleAttestationOfP3_te:roleAttestationR_?RoleOfP3_.
?RoleAttestationOfP3_te:roleAttestationR_te:TwsMo_.
#_To_display_the_TwsMO's role attestation
?RoleAttestationOfP3 te:roleAttestationR ?RoleOfP3.

# EvSP must be legally attested in its role
?RoleAttestationOfP2 te:raLegalQualification ?LegalRoleQualificationP2 .
# Display the legal norm itself for information purpose
?LegalRoleQualificationP2 te:legalQualificationN ?LegalNormP2.

# TwsMo must be legally attested in its role
#  TwsMo corresponds to ?P3issuerOfEvSProle, who has a role attestation ?RoleAttestationOfP3
?RoleAttestationOfP3 te:raLegalQualification ?LegalRoleQualificationP3 .
# Display the legal norm for information purpose
?LegalRoleQualificationP3 te:legalQualificationN ?LegalNormP3.
}
```

was implemented as described in Listing 13.14. The expected response is a list of all participants that are legally attested in their roles, with their legal qualification and the legal norm on which the legal qualification is based.

Rule $\beta_{IR3\text{-}D33\text{-}AP}$ (contained in Table 8.27) can be implemented by adding an additional condition to rule $\beta_{IR3\text{-}D32\text{-}AP}$. This condition requires that the evidence service provider's attestation of ISO/IEC TS 29003:2018 *Level of Identity Proofing 2* is attested by the trustworthiness monitor. Rule $\beta_{IR3\text{-}D33\text{-}AP}$ was implemented as described in Listing 13.15. The expected response is the list of participants that have a matching *Level of Identity Proofing* attestation. The trustor must verify whether the selected participant is included in the list.

Rule $\beta_{IR3\text{-}D34\text{-}AP}$ (contained in Table 8.28) can be implemented by changing the *Level of Identity Proofing* condition into *te:ISO-IEC-TS-29003:2018:LOIP3* in rule $\beta_{IR3\text{-}D33\text{-}AP}$.

13.6 IR4 Competently acting in role

13.6.1 Mandatory rules

The single mandatory rule $\beta_{IR4\text{-}M01}$ (the roles of a participant must be self-attested) is specified in Table 8.11. The rule was implemented as described in Listing 13.16. The expected response is

Listing 13.15: IR3-D33-AP

```
# IR3-D33-AP
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
# EvSP = ?P2issuerOfP1IdentityAttestation
# TwsMo = ?P3issuerOfEvSProle
?Participant1 rdf:type te:Participant .
?Participant1 rdf:type te:NaturalPerson .
?Participant1 te:pIdentityAttestation ?P1identityAttestation .
?P1identityAttestation prov:wasAttributedTo ?P2issuerOfP1IdentityAttestation.
?P2issuerOfP1IdentityAttestation te:pRoleAttestation ?RoleAttestationOfP2 .
?RoleAttestationOfP2 te:roleAttestationR te:EvSP .
# To display the EvSP's_role_attestation
?RoleAttestationOfP2_te:roleAttestationR_?RoleOfP2_.

#_EvSP_must_be_attested_by_TwsMo
?RoleAttestationOfP2_prov:wasAttributedTo_?P3issuerOfEvSProle_.
?P3issuerOfEvSProle_te:pRoleAttestation_?RoleAttestationOfP3_.
?RoleAttestationOfP3_te:roleAttestationR_te:TwsMo_.
#_To_display_the_TwsMO's role attestation
?RoleAttestationOfP3 te:roleAttestationR ?RoleOfP3.

# EvSP must be legally attested in its role
?RoleAttestationOfP2 te:raLegalQualification ?LegalRoleQualificationP2 .
# Display the legal norm for information purpose
?LegalRoleQualificationP2 te:legalQualificationN ?LegalNormP2.

# TwsMo must be legally attested in its role
#  TwsMo corresponds to ?P3issuerOfEvSProle, who has a role attestation ?RoleAttestationOfP3
?RoleAttestationOfP3 te:raLegalQualification ?LegalRoleQualificationP3 .
# Display the legal norm for information purpose
?LegalRoleQualificationP3 te:legalQualificationN ?LegalNormP3.

# Select conformance attestations of P1
?P2issuerOfP1IdentityAttestation te:pConformance ?IdentityAttestationConformance .
# Select only those conformance attestattions that come from the selected TwsMo
?IdentityAttestationConformance prov:wasAttributedTo ?P3issuerOfEvSProle .
# Select only those conformity attestations to match LOIP2
?IdentityAttestationConformance te:conformanceN te:ISO-IEC-TS-29003:2018:LOIP2 .
# Display the norm for information purpose
?IdentityAttestationConformance te:conformanceN ?IdentityNorm .

}
```

Listing 13.16: IR4-M01

```
# IR4-M01
# Roles must be self-attested
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX : <http://www.marcsel.eu/onto/te#>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
?Participant te:pRoleAttestation ?RoleAttestationOfParticipant .
    ?RoleAttestationOfParticipant prov:wasAttributedTo ?RoleAttestationAttributedTo .
    ?RoleAttestationOfParticipant prov:wasAttributedTo ?Participant .
}
```

Listing 13.17: IR4-D26-AP

```
# IR4-D26-AP
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
?P2issuerOfP1IdentityAttestation te:pRoleAttestation ?RoleAttestationOfP2 .
?RoleAttestationOfP2 te:roleAttestationR te:EvSP .
# that EvSP corresponds to ?P2issuerOfP1IdentityAttestation
#  which must be attested in its role by a trustworthiness monitor
?RoleAttestationOfP2 prov:wasAttributedTo ?P3issuerOfEvSProle .
?P3issuerOfEvSProle te:pRoleAttestation ?RoleAttestationOfP3 .
?RoleAttestationOfP3 te:roleAttestationR te:TwsMo .
# display the role that is attested explicitly
?RoleAttestationOfP3 te:roleAttestationR ?Role .
}
```

the list of participants that have self-attestations for their roles. The trustor must verify whether the selected participant is included in the list. An alternative implementation is possible by using the name of the selected participant.

13.6.2 Discretionary rules

A selection of IR4 discretionary rules was implemented. Rule $\beta_{IR4\text{-}D26\text{-}AP}$, described in Table 8.32, lists all evidence service providers attested in their role by a trustworthiness monitor. It was implemented as described in Listing 13.17. The expected response consists of a table of evidence service providers attested in their role by a trustworthiness monitor. The trustor must verify whether the selected participant is included in the list. An alternative implementation is possible by using the name of the selected participant.

Rule $\beta_{IR4\text{-}D027A\text{-}AP}$, also described in Table 8.32, lists all evidence service providers that are attested to their role by a trustworthiness monitor and that are listed in a European trust list. It was implemented as described in Listing 13.18. The expected response consists of a table of evidence service providers attested in their role by a trustworthiness monitor and listed in a European trust list[3]. The trustor must verify whether the selected participant is included in the

[3] As the only entities that are allowed to create entries in a European trust list are the registered trustworthiness monitors it is sufficient to verify the presence of evidence service providers in the European trust lists.

Listing 13.18: IR4-D027A-AP

```
# IR4-D027A-AP
# Lists evidence service providers included in a European trust list
# (limited to United Kingdom, Spain and Belgium)
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
?P2issuerOfP1IdentityAttestation te:pRoleAttestation ?RoleAttestationOfP2 .
?RoleAttestationOfP2 te:roleAttestationR te:EvSP .
# that EvSP corresponds to ?P2issuerOfP1IdentityAttestation
#  which must be included in a European trust list
?RoleAttestationOfP2 prov:wasDerivedFrom ?Source .
  FILTER (
       ?Source = <https://www.tscheme.org/sites/default/files/tsl-uk0022signed.xml> ||
       ?Source = <https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml> ||
       ?Source = <https://tsl.belgium.be/tsl-be.xml> ) .
}
```

Listing 13.19: IR4-D027B-AP

```
# IR4-D027B-AP
# Lists EvSPs that demonstrate compliance with ETSI EN 319 403
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
?Participant1 te:pRoleAttestation ?RoleAttestationOfP1 .
?RoleAttestationOfP1 te:roleAttestationR te:EvSP .
?Participant1 te:pConformance ?ConformanceAttestation .
?ConformanceAttestation te:conformanceN ?Standard .
  FILTER ( ?Standard = <http://www.marcsel.eu/onto/te/ETSI-EN-319-403> )
}
```

list. An alternative implementation is possible by using the name of the selected participant.

Rule $\beta_{IR4\text{-}D027B\text{-}AP}$, also described in Table 8.32, lists all evidence service providers that demonstrate conformance to ETSI EN 319 403 [88]. It was implemented as described in Listing 13.19. The expected response consists of a table of evidence service providers that demonstrate conformance to the standard. The trustor must verify whether the selected participant is included in the list. An alternative implementation is possible by using the name of the selected participant.

Rule $\beta_{IR4\text{-}D304\text{-}AP}$, described in Table 8.35, lists all evidence service providers that are monitored by a trustworthiness monitor that is legally attested to in this role. It was implemented as described in Listing 13.20. A similar rule for claim status service providers can be implemented by changing the role from evidence service provider to claim status service provider. The expected response consists of a list of evidence service providers that satisfy the condition. The trustor must verify whether the selected participant is included in the list. An alternative implementation is possible by using the name of the selected participant.

Listing 13.20: IR4-D304-AP

```
# IR4-D304-AP
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
# select evidence service providers that have evsp role attestation
?P1evsp te:pRoleAttestation ?RoleAttestationOfP1evsp .
?RoleAttestationOfP1evsp te:roleAttestationR te:EvSP .
#  EvSP must be supervised by TwsMo
?Supervision te:supervisionP ?P1evsp .
?P2twsmo te:pSupervision ?Supervision .
# TwsMo must be attested in its role
?P2twsmo te:pRoleAttestation ?RoleattestationOfP2twsmo .
?RoleattestationOfP2twsmo te:roleAttestationR te:TwsMo .
# TwsMo's_role_attestation_must_be_legally_qualified
?RoleattestationOfP2twsmo_te:raLegalQualification_?LegalRoleQualification_.
#_Display_the_legal_norm_for_information_purpose
?LegalRoleQualification_te:legalQualificationN_?LegalNorm.
}
```

13.7 Summary

This chapter presented a partial implementation of a specific rulebook, inspired by the European legislation for trust services. It complements the implementation of the data model and of the data import and transformation mechanism that were described in Chapters 11 and 12. The rules derived from requirements IR2 *Transparency* and IR3 *Linked and unique identity* together with a subset of those derived from IR4 *Competently acting in role* were implemented. The implementation also serves as a demonstration of how the rules for the other requirements can be implemented.

The approach, technical set-up and implementation of the rules was described. A similar approach can be applied to implement the remaining rules.

This implementation contributes to the validation of the proposed framework by showing how queries can demonstrate satisfaction of the FOL rules.

Chapter 14

Interpretation of trustworthiness

Building on the implementations of the data model, the data import and transformation functions, and the rulebook, the use of the trustworthiness evaluation function to improve the interpretation of trustworthiness is described.

14.1 Introduction

This chapter shows how the data that was collected and the rules that were specified in the previous chapters support the hypothesis of the thesis presented in Section 1.2.2. This hypothesis states that a reduction of possible interpretations of trust claims is desirable, and that such a reduction can be based on a systematic approach that combines collecting and aggregating trust artefacts that include contextual information, followed by reasoning according to clearly specified, documented and explainable logic. To support this hypothesis, the chapter presents:

- how rules can be selected from the rulebook specified in Chapter 13 to construct a trustworthiness evaluation function,
- how such a trustworthiness evaluation function can be executed using the database that was constructed in Chapter 12, and
- how the result obtained from performing this evaluation can be used to improve the interpretation of trustworthiness.

The remainder of this chapter is as follows.

- Section 14.2 describes the approach followed for performing trustworthiness evaluation.
- Section 14.3 describes the preparatory steps.

- Section 14.4 describes the evaluation of the mandatory rules. These rules are relevant regardless of the type of participant that is being evaluated.
- Section 14.5 describes the evaluation of an evidence service provider and how the results improve the interpretation of trustworthiness.
- Section 14.6 provides a summary of the chapter.

14.2 Approach

14.2.1 Overview

The proposed approach was introduced in Section 6.7.5 and consists of four steps.

- A choice must be made whether to evaluate the trustworthiness of an ecosystem or a participant.
  - In the ecosystem case, an ecosystem and a rulebook are evaluated without specifying a particular participant.
  - In the participant case, the participant that performs the evaluation is referred to as the potential trustor, and the participant whose data is evaluated is referred to as the potential trustee. The evaluation is performed in the context of a specific rulebook and database.

  Only the second case was implemented, since this allows a demonstration of the framework and the first case can be implemented in a similar way.
- A rulebook and a database containing instance data must be selected.
- Discretionary constraints must be selected from the chosen rulebook that correspond to the trustor's expectations regarding trustworthiness. These must be relevant to the trustor's decision to interact with the potential trustee. An example for an evidence service provider is described in Section 14.5.
- The ecosystem or participant trustworthiness evaluation function must be executed to determine whether the mandatory and the selected discretionary constraints can be satisfied by the selected instance data.

14.2.2 Performance

The evidence service provider was chosen as the class of participant for the demonstration of execution of trustworthiness evaluation. The reason for this choice is that participants in this class are instrumental in the provision of trust-related services. Furthermore, the implementation of trustworthiness evaluation for this class serves as a good example of how other participant classes can be evaluated. The company Zetes (te:Zetes-SA-NV) was selected as the evidence service provider to be evaluated.

To execute the $twseval_{AP}$ function, the potential trustor must execute the mandatory and selected discretionary queries. For the example policies that are described in this chapter, the results from the queries are described in Sections 14.4 and 14.5. Since this information consists of screenshots, the information cannot easily be presented here, so a summary is provided together with links to where full information can be obtained[1].

The results of the queries indicate whether the constraints are satisfied by the selected instance data. To interpret the results of the queries, the potential trustor can make use of the expected answers that are provided for each query in Chapter 13.

14.3 Preparatory steps

The potential trustor must access the file that contains the rulebook and the database that were developed. The potential trustor should perform the following steps.

- Calculate the RIPEMD-160 and/or SHA-256 digest(s) of the file that contains the rulebook, e.g. using CrypTool[2]. The file is available on-line[3].
- Retrieve the digest of the rulebook individual *te:RuleBook-001* specified by the property *te:ruleBook-digest-RIPEMD-160* and/or *te:ruleBook-digest-SHA-256* in the database[4].
- Verify that the respective digest values are identical; if so, the rulebook and the database are consistent and the potential trustor can proceed.

[1] To conduct a further test, a graph database can be installed and the *DBL.owl* file imported. The queries can be downloaded from the rulebook file (`http://www.marcsel.eu/onto/te/RuleBook-001.txt`) and can be executed over the data. The results of the queries can be consulted. Since all data is available in the database, the information resulting from the queries can be further navigated in the graph.

[2] `https://www.cryptool.org/en/`

[3] `http://www.marcsel.eu/onto/te/RuleBook-001.txt`

[4] `http://www.marcsel.eu/onto/te/DBL.owl`

14.4 Evaluation of the β_{AP} mandatory rules

A series of eight figures, described below, show the results obtained from executing a number of queries on the target database. These queries demonstrate the verification of the set of constraints specified in the mandatory rules of the input rulebook.

- Figure 14.1 shows the result of querying IR2-M01. This confirms that at least one rulebook is present in the database.
- Figure 14.2 shows the result of querying IR2-M02, the rulebook individual and its identifier.
- Additional to the information that results from the execution of the mandatory rules, rulebook information can be listed as follows.
  - Figure 14.3 shows the results from selecting the rulebook and shows the rulebook's properties.
  - Figure 14.4 shows the results from selecting the rulebook's identifier and shows its properties.
- Figure 14.5 shows a part of the result of querying IR2-M10 and lists a selection of the candidate participants. Zetes (te:Zetes-SA-NV) is included on line seven.
- Figure 14.6 shows a part of the result of querying IR3-M01 and lists a selection of the participants. Zetes is included on line six.

  Figure 14.7 shows the result of querying IR3-M01-EvSP. This refinement of IR3-M01 is described in Listing M.1. It adds the condition that the participant must be an EvSP to IR3-M01. Zetes is included on line two.
- Figure 14.8 shows the result of querying IR4-M01 and lists the participants that have self-attested role attestations. Zetes is included on line three.

Figure 14.1: The result of querying IR2-M01

	rulebook	id
1	te:RuleBook-001	te:ID-RuleBook-001

Figure 14.2: The result of querying IR2-M02

	subject	predicate	object
1	te:RuleBook-001	te:identifiedBy	te:ID-RuleBook-001
2	te:RuleBook-001	te:ruleBook-digest-RIPEMD-160	32 22 B5 E3 D3 E2 DC 4C A7 C0 7E 26 A9 3E B4 E3 F3 C4 15 77
3	te:RuleBook-001	te:ruleBook-digest-SHA-256	8B 3F 07 4A 99 9B C7 DE FB 5D C3 9E 94 05 98 AF 4C A1 90 52 D7 E5 64 D3 B8 4F 48 63 99 B6 45 03
4	te:RuleBook-001	rdf:type	te:RuleBook
5	te:RuleBook-001	rdf:type	owl:NamedIndividual
6	te:RuleBook-001	rdf:type	prov:Entity
7	te:RuleBook-001	rdfs:label	Rulebook 001
8	te:RuleBook-001	prov:wasAttributedTo	http://www.marcsel.eu/te/
9	te:RuleBook-001	prov:wasDerivedFrom	http://www.marcsel.eu/ti/manual
10	te:RuleBook-001	prov:wasGeneratedBy	http://www.marcsel.eu/ti/owl/DBL7.OWL.2021-01-02

Figure 14.3: Rulebook properties

	subject	predicate	object
1	te:ID-RuleBook-001	te:uniqueText	UUID-RuleBook-001
2	te:ID-RuleBook-001	rdf:type	te:ID
3	te:ID-RuleBook-001	rdf:type	owl:NamedIndividual
4	te:ID-RuleBook-001	rdfs:label	te:ID for RuleBook-001
5	te:ID-RuleBook-001	prov:wasAttributedTo	http://www.marcsel.eu/te/
6	te:ID-RuleBook-001	prov:wasDerivedFrom	http://www.marcsel.eu/ti/manual
7	te:ID-RuleBook-001	prov:wasGeneratedBy	http://www.marcsel.eu/ti/owl/DBL7.OWL.2021-01-02

Figure 14.4: Rulebook identifier properties

	Participant
1	te:participant-Alice
2	te:FPS-Economy-SMEs-Self-employed-and-Energy-Quality-and-Safety
3	te:Certipost-NV-SA
4	te:BE-BELAC
5	te:BE-AS-NRN
6	te:FR-COFRAC
7	te:Zetes-SA-NV
8	te:SMETS1-PKI-Service-from-SML
9	te:Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL
10	te:DigiCert-Europe-Belgium-BV
11	te:Portima-scrl-cvba
12	te:Connect-Solutions
13	te:Universign
14	te:Belgian-Mobile-ID-SA-NV
15	te:GlobalSign-NV-SA
16	te:SA-UNIFIEDPOST
17	te:Kingdom-of-Belgium-Federal-Government
18	te:MINISTERIO-DE-ECONOMIA-Y-EMPRESA
19	te:Banco-Santander-SA
20	te:Dirección-General-de-la-Policía
21	te:Agencia-Notarial-de-Certificación-SL-Unipersonal
22	te:Fábrica-Nacional-de-Moneda-y-Timbre-Real-Casa-de-la-Moneda-FNMT-RCM
23	te:Consorci-Administració-Oberta-de-Catalunya-CAOC
24	te:ANF-AUTORIDAD-DE-CERTIFICACION-ASOCIACION-ANF-AC
25	te:Consejo-General-de-la-Abogacía-Española
26	te:Colegio-de-Ingenieros-de-Caminos-Canales-y-Puertos
27	te:HEALTHSIGN-SL
28	te:Infraestructuras-y-Servicios-de-Telecomunicaciones-y-Certificación-SA
29	te:AC-Camerfirma-SA
30	te:COLEGIO-OFICIAL-DE-REGISTRADORES-DE-LA-PROPIEDAD-Y-MERCANTILES-DE-ESPAÑA
31	te:Banco-Español-de-Crédito-SA
32	te:EDICOM-CAPITAL-SL
33	te:Autoridad-de-Gestión-de-la-PKI-del-Ministerio-de-Defensa-AGPMD-y-Director-del-CESTIC-Centro-de-Sistemas-y-Tecnologías-de-la-Información-y-las-Comunicaciones-CESTIC
34	te:Ziurtapen-eta-Zerbitzu-Enpresa-Empresa-de-Certificación-y-Servicios-Izenpe-SA
35	te:Firmaprofesional-SA
36	te:Tesorería-General-de-la-Seguridad-Social
37	te:Ministerio-de-Empleo-y-Seguridad-Social

Figure 14.5: The result of querying IR2-M10, a list of candidate participants (selection)

14.5 Evidence service provider

Three EvSP trustworthiness policies were created to serve as examples of the policy types that can be specified. Their evaluations provide results that allow the potential trustor to evaluate a potential trustee (Zetes) in the role of an evidence service provider. The example policies are described as well as the expected and actual query results.

14.5.1 First EvSP trustworthiness policy

The first policy requires that the potential trustee:

- has a self-attested EvSP role attestation (IR3-D11-AP), and
- has an EvSP role attestation issued by a trustworthiness monitor (IR4-D26-AP).

14.5.2 Evaluation results

The results of the execution of the corresponding rules on the *DBL.owl* database are shown in the following figures.

- Figure 14.9 shows the result of querying IR3-D11-AP . The expected result is that the potential trustee is included in the list[5].
- Figure 14.10 shows the result of querying IR4-D26-AP. The expected result is that the potential trustee is included in the list. Zetes is included on line three.

14.5.3 Second EvSP trustworthiness policy

The second policy requires that the potential trustee:

- has a legal attestation of its role (IR4-D304B-AP), and
- has a role attestation based on a European trust list (IR4-D027A-AP).

14.5.4 Evaluation results

The results of the execution of the corresponding rules on the *DBL.owl* database are shown in the following figures.

- Figure 14.11 shows the result of querying the query IR4-D304B-AP and lists all evidence service providers that are legally attested in their role. The expected result is that the potential trustee is included in the list. Zetes is included on line two.

  This list might omit some evidence service providers that are legally attested in their role. The database contains 70 evidence service providers, generated by the XSL programs on the basis of the public trusted lists. The database contains two legal attestations for evidence service providers only. The reason is that there is no obligation or common

[5]Natural persons with FOAF data do not appear in the list. This is because their attestations are based on the Mendeley dataset, rather than on the participants themselves.

way for evidence service providers to operate under a legal mandate that could be used as a basis for *te:Legal Qualification*. As a consequence, legal attestations have to be investigated on an individual basis.

Additional information can be obtained as follows.

- Figure 14.12 shows all participants for which a legal attestation was created on the basis of a legal document. This was implemented as described in Listing M.2. Zetes is included on line six.
- Figure 14.13 shows a selection of the sources from where role attestations were derived. This was implemented as described in Listing M.3. Zetes is included on line four.

- Figure 14.14 shows the result of querying the query IR4-D027A-AP and lists all evidence service providers included in a European trust list (limited to the United Kingdom, Spain and Belgium). The expected result is that the potential trustee is included in the list. The list has 69 entries. Zetes is included on line 60.

14.5.5 Third EvSP trustworthiness policy

The third policy requires that the evidence service provider has a conformity attestation for ETSI EN 319 403 [87] (IR4-D027B), and illustrates the possibility of additional conformity attestation regarding further ETSI standards related to electronic trust services. There are more than 100 such ETSI standards that can be consulted on the ETSI portal[6].

14.5.6 Evaluation results

Figure 14.15 shows the result of querying the query IR4-D027B and lists all evidence service providers that demonstrate compliance with ETSI EN 319 403 [87]. The expected result is that the potential trustee is included in the list. Zetes is not included in the list.

Figure 14.16 shows all participants for which a conformance attestation was created on the basis of the information published by a conformity assessment body. This was implemented as described in Listing M.4. Standards that are commonly in use include:

- ETSI EN 319 401 [91],
- ETSI EN 319 411-1 [93], and
- ETSI EN 319 411-2 [95].

[6] `https://portal.etsi.org/home.aspx`

The expected result is that the evidence service provider that was selected as potential trustee demonstrates a conformity attestation of the standards that the potential trustor identified as relevant. Zetes is included in the list on lines one, two and three.

	participant	id
1	tc:FPS-Economy-SMEs-Self-employed-and-Energy-Quality-and-Safety	tc:ID-FPS-Economy-SMEs-Self-employed-and-Energy-Quality-and-Safety
2	tc:Certipost-NV-SA	tc:ID-Certipost-NV-SA
3	tc:BE-BELAC	tc:ID-BE-BELAC
4	tc:BE-AS-NRN	tc:ID-BE-AS-NRN:1983-08-08-1984021127
5	tc:FR-COFRAC	tc:ID-AB-FR-COFRAC
6	tc:Zetes-SA-NV	tc:ID-Zetes-SA-NV
7	tc:SMETS1-PKI-Service-from-SML	tc:ID-SMETS1-PKI-Service-from-SML
8	tc:Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL	tc:ID-Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL
9	tc:DigiCert-Europe-Belgium-BV	tc:ID-DigiCert-Europe-Belgium-BV
10	tc:Portima-scrl-cvba	tc:ID-Portima-scrl-cvba
11	tc:Connect-Solutions	tc:ID-Connect-Solutions
12	tc:Universign	tc:ID-Universign
13	tc:Belgian-Mobile-ID-SA-NV	tc:ID-Belgian-Mobile-ID-SA-NV
14	tc:GlobalSign-NV-SA	tc:ID-GlobalSign-NV-SA
15	tc:SA-UNIFIEDPOST	tc:ID-SA-UNIFIEDPOST
16	tc:Kingdom-of-Belgium-Federal-Government	tc:ID-Kingdom-of-Belgium-Federal-Government
17	tc:MINISTERIO-DE-ECONOMIA-Y-EMPRESA	tc:ID-MINISTERIO-DE-ECONOMIA-Y-EMPRESA
18	tc:Banco-Santander-SA	tc:ID-Banco-Santander-SA
19	tc:Dirección-General-de-la-Policía	tc:ID-Dirección-General-de-la-Policía

Figure 14.6: The result of querying IR3-M01, the list of participants (selection)

	Participant	Role
1	te:Certipost-NV-SA	te:EvSP
2	te:Zetes-SA-NV	te:EvSP
3	te:SMETSI-PKI-Service-from-SML	te:EvSP
4	te:Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL	te:EvSP
5	te:DigiCert-Europe-Belgium-BV	te:EvSP
6	te:Portima-scrl-crba	te:EvSP
7	te:Connect-Solutions	te:EvSP
8	te:Universign	te:EvSP
9	te:Belgian-Mobile-ID-SA-NV	te:EvSP
10	te:GlobalSign-NV-SA	te:EvSP
11	te:SA-UNIFIEDPOST	te:EvSP
12	te:Kingdom-of-Belgium-Federal-Government	te:EvSP
13	te:Banco-Santander-SA	te:EvSP
14	te:Dirección-General-de-la-Policía	te:EvSP
15	te:Agencia-Notarial-de-Certificación-SL-Unipersonal	te:EvSP
16	te:Fábrica-Nacional-de-Moneda-y-Timbre-Real-Casa-de-la-Moneda-FNMT-RCM	te:EvSP
17	te:Consorci-Administració-Oberta-de-Catalunya-CAOC	te:EvSP
18	te:ANF-AUTORIDAD-DE-CERTIFICACIÓN-ASOCIACIÓN-ANF-AC	te:EvSP
19	te:Consejo-General-de-la-Abogacía-Española	te:EvSP
20	te:Colegio-de-Ingenieros-de-Caminos-Canales-y-Puertos	te:EvSP
21	te:HEALTHSIGN-SL	te:EvSP
22	te:Infraestructuras-y-Servicios-de-Telecomunicaciones-y-Certificación-SA	te:EvSP
23	te:AC-Camerfirma-SA	te:EvSP
24	te:COLEGIO-OFICIAL-DE-REGISTRADORES-DE-LA-PROPIEDAD-Y-MERCANTILES-DE-ESPAÑA	te:EvSP
25	te:Banco-Español-de-Crédito-SA	te:EvSP
26	te:EDICOM-CAPITAL-SL	te:EvSP

Figure 14.7: The result of querying IR3-M01-EvSP, a list of EvSP participants and their role (selection)

	Participant	RoleAttestationOfParticipant	RoleAttestationAttributedTo
1	te:FPS-Economy-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:FPS-Economy-SMEs-Self-employed-and-Energy-Quality-and-Safety
2	te:Certipost-NV-SA	te:RoleAttestation-Certipost-NV-SA-self	te:Certipost-NV-SA
3	te:Zetes-SA-NV	te:RoleAttestation-Zetes-SA-NV-self	te:Zetes-SA-NV
4	te:SMETS1-PKI-Service-from-SML	te:RoleAttestation-SMETS1-PKI-Service-from-SML-self	te:SMETS1-PKI-Service-from-SML
5	te:MINISTERIO-DE-ECONOMIA-Y-EMPRESA	te:RoleAttestation-TwsMo-MINISTERIO-DE-ECONOMIA-Y-EMPRESA	te:MINISTERIO-DE-ECONOMIA-Y-EMPRESA
6	te:tScheme-Limited	te:RoleAttestation-TwsMo-tScheme-Limited	te:tScheme-Limited
7	te:European-Commission	te:RoleAttestation-TwsMo-European-Commission	te:European-Commission

Figure 14.8: The result of querying IR4-M01, a list of participants that have self-attested role-attestations

	Participant	identityAttestation	issuerOfIdentityAttestation
1	te:FPS-Economy:-SMEs-Self-employed-and-Energy:-Quality-and-Safety	te:Identity-Attestation-FPS-Economy:-SMEs-Self-employed-and-Energy:-Quality-and-Safety	te:FPS-Economy:-SMEs-Self-employed-and-Energy:-Quality-and-Safety
2	te:Certpost-NV-SA	te:Identity-Attestation-Certpost-NV-SA-self	te:Certpost-NV-SA
3	te:Zetes-SA-NV	te:Identity-Attestation-Zetes-SA-NV-self	te:Zetes-SA-NV
4	te:SMETS1-PKI-Service-from-SML	te:Identity-Attestation-SMETS1-PKI-Service-from-SML-self	te:SMETS1-PKI-Service-from-SML
5	te:MINISTERIO-DE-ECONOMIA-Y-EMPRESA	te:Identity-Attestation-MINISTERIO-DE-ECONOMIA-Y-EMPRESA	te:MINISTERIO-DE-ECONOMIA-Y-EMPRESA
6	te:tScheme-Limited	te:Identity-Attestation-tScheme-Limited	te:tScheme-Limited
7	te:European-Commission	te:Identity-Attestation-European-Commission	te:European-Commission

Figure 14.9: The result of querying IR3-D11-AP, a list of participants and their self-attested identity attestations (selection)

	P2issuerOfP1IdentityAttestation	RoleAttestationOfP2	P3issuerOfEvSProle	RoleAttestationOfP3	Role
1	te:Certipost-NV-SA	te:RoleAttestation-Certipost-NV-SA	te:FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:TwsMo
2	te:Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL	te:RoleAttestation-Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL	te:FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:TwsMo
3	te:DigiCert-Europe-Belgium-BV	te:RoleAttestation-DigiCert-Europe-Belgium-BV	te:FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:TwsMo
4	te:Zetes-SA-NV	te:RoleAttestation-Zetes-SA-NV	te:FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:TwsMo
5	te:Portima-scrl-cvba	te:RoleAttestation-Portima-scrl-cvba	te:FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:TwsMo
6	te:Connect-Solutions	te:RoleAttestation-Connect-Solutions	te:FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:TwsMo
7	te:Universign	te:RoleAttestation-Universign	te:FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:TwsMo
8	te:Belgian-Mobile-ID-SA-NV	te:RoleAttestation-Belgian-Mobile-ID-SA-NV	te:FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:TwsMo
9	te:GlobalSign-NV-SA	te:RoleAttestation-GlobalSign-NV-SA	te:FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:TwsMo
10	te:SA-UNIFIEDPOST	te:RoleAttestation-SA-UNIFIEDPOST	te:FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy:-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:TwsMo

Figure 14.10: The result of querying IR4-D26-AP, the EvSPs attested in their role by a TwsMo (selection)

	PIevsp	RoleAttestationOfPIevsp	LegalRoleQualification	LegalNorm
1	te:Certipost-NV-SA	te:RoleAttestation-Certipost-NV-SA	te:BE-LegalQualification-003	te:BE-Certipost-CitizenCA-CPS-Version-1.4
2	te:Zetes-SA-NV	te:RoleAttestation-Zetes-SA-NV	te:BE-LegalQualification-007	te:BE-Zetes-CitizenCA-ForeignerCA-CP-CPS-Version-1.1

Figure 14.11: The result of querying IR4-D304B-AP, the list of EvSPs legally attested in their role and their legal norm

	PIevsp	RoleAttestationOfPIevsp	LegalRoleQualification	LegalNorm
1	te:BE-BELAC	te:RoleAttestation-AB-BE-BELAC	te:BE-LegalQualification-001	te:BE-Royal-Decree-BELAC-D2014-02-07
2	te:Certipost-NV-SA	te:RoleAttestation-Certipost-NV-SA	te:BE-LegalQualification-003	te:BE-Certipost-CitizenCA-CPS-Version-1.4
3	te:FR-COFRAC	te:RoleAttestation-AB-FR-COFRAC	te:FR-LegalQualification-001	https://www.legifrance.gouv.fr/loda/id/JORFTEXT000019992087/
4	te:FPS-Economy-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:BE-LegalQualification-004	te:BE-LAW-FPS-ECO-BE-SIGN-establishment-2016
5	te:UK-UKAS	te:RoleAttestation-AB-UK-UKAS	te:UK-LegalQualification-001	https://www.legislation.gov.uk/uksi/2009/3155/pdfs/uksi_20093155_en.pdf
6	te:Zetes-SA-NV	te:RoleAttestation-Zetes-SA-NV	te:BE-LegalQualification-007	te:BE-Zetes-CitizenCA-ForeignerCA-CP-CPS-Version-1.1

Figure 14.12: Additional information: the list of all participants legally attested in their role

	EvSP	RoleAttestation	wasDerivedFrom
1	te:Certipost-NV-SA	te:RoleAttestation-Certipost-NV-SA	https://tsl.belgium.be/tsl-be.xml
2	te:Zetes-SA-NV	te:RoleAttestation-Zetes-SA-NV	https://tsl.belgium.be/tsl-be.xml
3	te:Certipost-NV-SA	te:RoleAttestation-Certipost-NV-SA-self	https://www.basware.com/en-en/about-basware/legacy-of-innovation/
4	te:Zetes-SA-NV	te:RoleAttestation-Zetes-SA-NV-self	https://www.zetes.com/en
5	te:SMETS1-PKI-Service-from-SML	te:RoleAttestation-SMETS1-PKI-Service-from-SML-self	https://www.securemeters.com/
6	te:Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL	te:RoleAttestation-Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL	https://tsl.belgium.be/tsl-be.xml
7	te:DigiCert-Europe-Belgium-BV	te:RoleAttestation-DigiCert-Europe-Belgium-BV	https://tsl.belgium.be/tsl-be.xml
8	te:Portima-scrl-cvba	te:RoleAttestation-Portima-scrl-cvba	https://tsl.belgium.be/tsl-be.xml
9	te:Connect-Solutions	te:RoleAttestation-Connect-Solutions	https://tsl.belgium.be/tsl-be.xml
10	te:Universign	te:RoleAttestation-Universign	https://tsl.belgium.be/tsl-be.xml
11	te:Belgian-Mobile-ID-SA-NV	te:RoleAttestation-Belgian-Mobile-ID-SA-NV	https://tsl.belgium.be/tsl-be.xml
12	te:GlobalSign-NV-SA	te:RoleAttestation-GlobalSign-NV-SA	https://tsl.belgium.be/tsl-be.xml
13	te:SA-UNIFIEDPOST	te:RoleAttestation-SA-UNIFIEDPOST	https://tsl.belgium.be/tsl-be.xml
14	te:Kingdom-of-Belgium-Federal-Government	te:RoleAttestation-Kingdom-of-Belgium-Federal-Government	https://tsl.belgium.be/tsl-be.xml
15	te:Banco-Santander-SA	te:RoleAttestation-Banco-Santander-SA	https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml
16	te:Dirección-General-de-la-Policía	te:RoleAttestation-Dirección-General-de-la-Policía	https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml
17	te:Agencia-Notarial-de-Certificación-SL-Unipersonal	te:RoleAttestation-Agencia-Notarial-de-Certificación-SL-Unipersonal	https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml
18	te:Fábrica-Nacional-de-Moneda-y-Timbre-Real-Casa-de-la-Moneda-FNMT-RCM	te:RoleAttestation-Fábrica-Nacional-de-Moneda-y-Timbre-Real-Casa-de-la-Moneda-FNMT-RCM	https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml
19	te:Consorci-Administració-Oberta-de-Catalunya-CAOC	te:RoleAttestation-Consorci-Administració-Oberta-de-Catalunya-CAOC	https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml

Figure 14.13: Additional information: the list of EvSPs and the sources of their role attestation (selection)

47	te:Logalty-Prueba-por-Interposición-SL	te:RoleAttestation-Logalty-Prueba-por-Interposición-SL	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
48	te:LLEIDANETWORKS-SERVEIS-TELEMATICS-SA	te:RoleAttestation-LLEIDANETWORKS-SERVEIS-TELEMATICS-SA	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
49	te:BRANDDOCS-SL	te:RoleAttestation-BRANDDOCS-SL	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
50	te:Ecertic-Digital-Solutions-SL	te:RoleAttestation-Ecertic-Digital-Solutions-SL	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
51	te:DIGITEL-ON-TRUSTED-SERVICES-SLU.	te:RoleAttestation-DIGITEL-ON-TRUSTED-SERVICES-SLU.	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
52	te:VIAFIRMA-SL	te:RoleAttestation-VIAFIRMA-SL	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
53	te:VALIDATED-ID-SL	te:RoleAttestation-VALIDATED-ID-SL	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
54	te:Entrust-Datacard-Europe-SLU.	te:RoleAttestation-Entrust-Datacard-Europe-SLU.	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
55	te:EVIDENCIAS-CERTIFICADAS-SL	te:RoleAttestation-EVIDENCIAS-CERTIFICADAS-SL	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
56	te:EAD-TRUST-European-Agency-of-Digital-Trust-SL	te:RoleAttestation-EAD-TRUST-European-Agency-of-Digital-Trust-SL	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
57	te:Bewor-tech-SL	te:RoleAttestation-Bewor-tech-SL	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
58	te:ELECTRONIC-IDENTIFICATION-SL	te:RoleAttestation-ELECTRONIC-IDENTIFICATION-SL	https://sede.minetur.gob.es Prestadores/TSL/TSL.xml
59	te:Certipost-NV-SA	te:RoleAttestation-Certipost-NV-SA	https://tsl.belgium.be/tsl-be.xml
60	te:Zetes-SA-NV	te:RoleAttestation-Zetes-SA-NV	https://tsl.belgium.be/tsl-be.xml
61	te:Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL	te:RoleAttestation-Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL	https://tsl.belgium.be/tsl-be.xml

Figure 14.14: The result of querying IR4-D027A-AP, the list of EvSPs included in a European trust list (selection)

	Participant1	RoleAttestationOfP1	ConformanceAttestation	Standard
1	te:British-Telecommunications-Plc	te:RoleAttestation-British-Telecommunications-Plc	te:LSTI-BT-ConformanceAttestation-001	te:ETSI-EN-319-403

Figure 14.15: The result of querying IR4-D027B, the list of EvSPs that demonstrate compliance with ETSI EN 319 403 [87]

	P1	ConformanceAttestationOfP1	Standard
1	te:Zetes-SA-NV	te:LSTI-ZETES-ConformanceAttestation-001	te:ETSI-EN-319-401
2	te:Zetes-SA-NV	te:LSTI-ZETES-ConformanceAttestation-001	te:ETSI-EN-319-411-1
3	te:Zetes-SA-NV	te:LSTI-ZETES-ConformanceAttestation-001	te:ETSI-EN-319-411-2
4	te:British-Telecommunications-Plc	te:LSTI-BT-ConformanceAttestation-001	te:ETSI-EN-319-401
5	te:British-Telecommunications-Plc	te:LSTI-BT-ConformanceAttestation-001	te:ETSI-EN-319-403
6	te:British-Telecommunications-Plc	te:LSTI-BT-ConformanceAttestation-001	te:ETSI-EN-319-411-1
7	te:CertSIGN-SA	te:LSTI-CertSIGN-ConformanceAttestation-001	te:ETSI-EN-319-401
8	te:CertSIGN-SA	te:LSTI-CertSIGN-ConformanceAttestation-001	te:ETSI-EN-319-403
9	te:CertSIGN-SA	te:LSTI-CertSIGN-ConformanceAttestation-001	te:ETSI-EN-319-411-1
10	te:CertSIGN-SA	te:LSTI-CertSIGN-ConformanceAttestation-001	te:CABForum-EV-SSL-Certificate-Guidelines-v1.7.1
11	te:Dhimyotis	te:LSTI-Dhimyotis-ConformanceAttestation-001	te:ETSI-EN-319-401
12	te:Dhimyotis	te:LSTI-Dhimyotis-ConformanceAttestation-001	te:ETSI-EN-319-403
13	te:Dhimyotis	te:LSTI-Dhimyotis-ConformanceAttestation-001	te:ETSI-EN-319-411-1
14	te:Dhimyotis	te:LSTI-Dhimyotis-ConformanceAttestation-001	te:ETSI-EN-319-411-2
15	te:Dhimyotis	te:LSTI-Dhimyotis-ConformanceAttestation-001	te:CABForum-EV-SSL-Certificate-Guidelines-v1.7.1
16	te:Dhimyotis	te:LSTI-Dhimyotis-ConformanceAttestation-001	te:ETSI-EN-119-403-2
17	te:E-Tugra	te:LSTI-E-Tugra-ConformanceAttestation-001	te:ETSI-TS-119-403-2
18	te:E-Tugra	te:LSTI-E-Tugra-ConformanceAttestation-001	te:ETSI-EN-319-401
19	te:E-Tugra	te:LSTI-E-Tugra-ConformanceAttestation-001	te:ETSI-EN-319-403-1
20	te:E-Tugra	te:LSTI-E-Tugra-ConformanceAttestation-001	te:ETSI-EN-319-411-1
21	te:E-Tugra	te:LSTI-E-Tugra-ConformanceAttestation-001	te:CABForum-EV-SSL-Certificate-Guidelines-v1.7.1

Figure 14.16: The result of querying IRX-Participants-conformance, the list of participants with an attestation of conformance to a standard

14.6 Summary

This chapter presented results from performing the prototype implementation of the trustworthiness evaluation function on selected test data. The approach, consisting of four steps, was described. The implementation of the function $twseval_{AP}$ for the participant class of evidence service provider was provided. This allows the evaluation of a specific participant of the class evidence service provider as potential trustee. Three EvSP trustworthiness policies were created to serve as examples of the policy types that can be specified. Their evaluations provide results that allow a potential trustor to evaluate a potential trustee in the role of an evidence service provider. The example policies were described as well as the expected and actual query results. This contributes to the validation of the proposed framework by showing

- how a potential trustor can select discretionary rules from a rulebook to specify a policy for trustworthiness evaluation,
- how the corresponding queries can be performed, and
- how the results demonstrate satisfaction (or the lack thereof) of the selected rules, which assists in the evaluation of a potential trustee.

Chapter 15

Results and comparison with prior art

This chapter presents experimental results obtained from the partial implementation and a comparison with the prior art.

15.1 Introduction

This chapter presents experimental results obtained from the partial implementation described in Chapters 10 – 13. A comparison with the prior art is also provided. The remainder of this chapter is structured as follows.

- Section 15.2 provides experimental results from the partial implementation of the $\mathcal{TE}$ framework on a laptop computer.
- Section 15.3 provides a comparison with the prior art.
- Section 15.4 provides a summary of the chapter.

15.2 Experimental results

A laptop computer was used for the implementation of the $\mathcal{TE}$ framework. This laptop was running the Windows 10 64-bit Operating System and equipped with an Intel(R) Core(TM) i7-4700 MQ CPU, running at 2.4 GHz, and with 12 GB ram.

Downloading the data sources employed a home-office Internet connection using the Digital Subscriber Line (DSL) protocol. The network speed was measured using the ISP's speedtest and indicated a download speed of 20.9 Mbps (and an upload speed of 5.5 Mbps).

The Trusted Lists that were selected vary in size between 338 Kilobytes and 2162 Kilobytes. Each individual download took less than one second. Extracting the selected data for 100.000 organisations from the FactForge SPARQL endpoint took 0.2 seconds, and the download took

less than one second. The Mendeley Data's FOAF dataset has a size of 3 Megabytes and was downloaded in less than one second.

The execution of the XSL transformation on the laptop was performed while no other applications were active. Their execution always took less than one second. The following values are listed as examples.

- TL2RDF_DataSource_LOTL_v301 took 385 milliseconds.
- TL2RDF_UK_EvSPs_v301 took 495 milliseconds.
- TL2RDF_BE_TwsMo_v301 took 426 milliseconds.
- FOAF_01_NP_v301 took 431 milliseconds.
- FOAF_02_NP_v301 took 524 milliseconds.

The creation of the database load file *DBL.owl* is described in Appendix L. Its loading in the GraphDB database took approximately one second. A data import results in a total of 10787 statements in the database, of which 6250 are explicit assertions and 4537 are inferred. The execution of the SPARQL queries took between 20 and 100 milliseconds.

Comparable performance figures for the prior art approaches described in Section 15.3 could not be identified.

15.3 Comparison with prior art

A comparison with the prior art was performed by analysing how the proposed $\mathcal{TE}$ framework approach relates to commonly accepted trust concepts, including those defined by Marsh and by Bacharach and Gambetta, and by comparing it to the approaches of PKI, the Web of Trust and selected other trust-related ontologies.

15.3.1 Preliminary observations

The proposed $\mathcal{TE}$ framework is aligned with the following well-established principles related to trust.

- It aligns with Luhmann's thesis, as expressed in his work *Trust and Power* [226], that 'trust allows to reduce the complexity of society' by introducing a set of specialised roles, and then introducing a formalisation for the qualification of these roles.
- It aligns with the concept of segregation of duty, specified by Clark and Wilson [60], by introducing roles and constraints related to which roles can be combined.

15.3.2 Relationship to Marsh's concepts

As discussed in Section 2.3.2, Marsh [234] proposed formalising trust as a computational concept. His proposals are relevant to evaluating trustworthiness in an electronic society, and are hence relevant to the problems addressed in the thesis. The concepts of Marsh are related to the $\mathcal{TE}$ framework in the following ways.

- In Marsh's approach, the trustor and trustee are referred to as 'agents' and it is implicitly assumed they exist and are uniquely defined. It is also assumed agents have access to information about other agents and the situations. However, how such information should be specified and used is not formally defined.

  To refer more concretely to these agents and to specify constraints on them, the $\mathcal{TE}$ framework contains rules ensuring the existence and uniqueness of participants.

- Marsh identifies situational trust, which corresponds to trust of x in y for z. He gives the example of trusting his brother for driving him to the airport but not for flying the plane.

  In the $\mathcal{TE}$ framework, this is captured in the data model, more particularly in the set of roles.

15.3.3 Relationship to Bacharach and Gambetta

15.3.3.1 The underlying problems of trust

As discussed in Section 2.2.1, Bacharach and Gambetta [18] describe what they refer to as 'the underlying problems of trust' and introduce a distinction between the primary and secondary problems of trust. These notions relate to the $\mathcal{TE}$ framework in the following ways.

- The primary problem addressed by Bacharach and Gambetta is whether one can trust a person to do X. This can be evaluated in two ways.

  - Directly, in which case the person simply 'does X'. This case is disregarded by Bacharach and Gambetta since it ignores the trust-related decision altogether, and completely exposes the trustor to the trustee. This case is also disregarded in the $\mathcal{TE}$ framework.
  - Indirectly, based on information gathered from the context. In the $\mathcal{TE}$ framework this is addressed by attestations, either self-provided or provided by another participant.

- The secondary problem is how to construct sufficiently clear identities for the person and X. This is addressed by the data model described in Chapter 7 and the constraints described in Chapter 8.

Building on the work of Bacharach and Gambetta, we formulate a third underlying problem of trust as whether to rely on a trust evaluation performed by oneself or by another party.

15.3.3.2 Addressing the underlying problems of trust

The three problems discussed above are addressed in the $\mathcal{TE}$ framework in the following ways.

- The primary problem of trust, whether one can trust a person to do *X*, is addressed by the use of attestations.
- The second problem, how to construct sufficiently clear identies of the person and *X*, is addressed by the data model described in Chapter 7 and the constraints described in Chapter 8.
- The third problem, whether to rely on a trust evaluation performed by oneself or by another party, currently remains unaddressed. However, it could be addressed by explicitly describing and evaluating the evaluator (as 'evaluated by'). This is not covered in the framework as currently defined, and addressing this is a possible area for future research. An outline of how it could be addressed is provided in Section 16.4.5.

15.3.4 PKI

PKI, whose trust model was introduced in Section 2.3.2, was chosen as a basis for validation because it is a trust model that is in use today on a global scale. This focus is supported by the recent ETSI report TR 103 684 [99] on global trust which states that it concentrates on existing PKI-based trust services as these are the most prevalent across the world. PKI and its trust model were described in Section 2.3. We argue the proposed $\mathcal{TE}$ framework is more precise than PKI in terms of semantics regarding the meaning of trustworthiness for the following reasons.

- PKI policies suffer from a lack of clear semantics. This was observed in the survey as described in Section 3.5.2.5 and analysed in Section 3.5.3.1.
- The ETSI report TR 103 684 [99] analyses 37 PKI standard, global, sector and national PKI schemes. Part of the study addresses trust representation. The study states that the following four main models for representation of trust are widely used:
  - national root-signing by a national root CA with the ability to cross-certify other CAs for recognition;
  - trust stores listing the approved issuing CAs or root-CAs operated by an application or software platform provider;

- trusted lists as specified in ETSI TS 119 612 [89]; and
- cross certification between CAs, or between a CA and a root-CA, through a bridge CA.

However these four models are not models for representation of trust but rather models to specify anchor points for the trust required in a PKI root.

We argue that the semantic approach proposed in the $\mathcal{TE}$ framework is more complete and semantically more precise in representing and reasoning about trust, because it allows a potential trustor to select data points that represent information on a potential trustee from a qualified and distributed set of data sources. Furthermore the PKI model does not allow the role and potential trustworthiness of the service provider that verifies the status of an authenticated or signed object to be clearly described. The traditional PKI role distribution is as follows:

- an entity registers with a Certification Authority, which accepts the entity according its policy;
- as a result of acceptance the entity receives one or more certificates;
- the entity can then use these certificates to engage in an interaction with a relying party;
- the replying party can then validate aspects of the interaction (e.g. verifying a public key or an attribute) using the certificates.

What is rarely if ever addressed in PKI policies is the fact that, if the verification policy is complex in nature, verification may involve another service provider. Such a service provider is explicitly introduced in the $\mathcal{TE}$ data model as the claim status service provider.

15.3.5 Web of Trust

As described in Section 6.2.1, the PGP Web of Trust is an alternative to a conventional PKI and is used extensively, but it lacks precise semantics. We argue that the $\mathcal{TE}$ framework is more precise regarding the meaning of trustworthiness for the following reasons.

- PGP creates a graph of interrelationships by letting users sign keys they consider trustworthy. However PGP lacks a mechanism to extend this graph with any other attributes.

  The $\mathcal{TE}$ framework allows a more granular specification of the interrelationships through its use of attestations.

- PGP lacks a mechanism for propagating trust opinions within the web of trust.

  Following Marsh (see Section 3.5.3.2) the $\mathcal{TE}$ framework does not assume that trust is transitive. However, the $\mathcal{TE}$ framework offers an alternative in the form of chaining of relationships, such as in the rule $\beta_{IR4-D026}$. It is possible to evaluate chains of edges such as those created by the relationships between accreditation bodies, conformity assessment bodies and evidence service providers.

15.3.6 Trust-related ontologies

The survey in Chapter 3 classified trust-related approaches into five clusters. Of these approaches, those that appear in the cluster 'trust-related ontologies specified in OWL' are compared below to the $\mathcal{TE}$ framework because their objectives, representation formalisms and reasoning mechanism are the closest to it. This cluster is described in Section 3.5.2.1, and Table 3.1 provides an overview.

15.3.6.1 Bernabé et al. – SOFIC/Trust-DSS

Bernabé et al. [26] proposed a Security Ontology For the InterCloud (SOFIC). The $\mathcal{TE}$ framework relates to the SOFIC/Trust-DSS system in the following ways.

- Similarities include the following.
  - Both use the formalisms of an ontology and rules with the aim to support trust-related decisions.
  - Both import other ontologies to improve interoperability.
- The following are the main differences.
  - SOFIC/Trust-DSS approach focuses on decisions related to cloud service providers while the $\mathcal{TE}$ framework addresses the broader setting of a potential trustor and a potential trustee.
  - The SOFIC/Trust-DSS approach bases its trust-related decision support on an ontology which is security based. The $\mathcal{TE}$ data model integrates security data points but is not limited to them.
  - The SOFIC/Trust-DSS approach involves significant manual effort for translation of observations about service providers into instances of a SOFIC class, and for the customisation of rules to express what needs to be assessed. The $\mathcal{TE}$ framework has automated this translation by the use of XSL, and includes the concept of a rulebook which consists of pre-specified rules.

- The SOFIC/Trust-DSS approach is open to a variety of data sources and rules may be created for specific cases. The operation of the $\mathcal{TE}$ framework has been demonstrated using real-world data imported through the data import and transformation mechanism, which outputs the data expressed using description logic.
- The SOFIC/Trust-DSS approach uses data aggregation and quantification. The $\mathcal{TE}$ framework does not, because we argued in Section 3.5.3.2 that it is not useful for trust.

15.3.6.2 Karthik and Ananthanarayana – the TRUST framework

Karthik and Ananthanarayana [197] proposed a trust framework for sensor-driven pervasive environments that is based on an OWL ontology and security rules in SWRL. The ontology is referred to as the TRUST ontology. The $\mathcal{TE}$ framework relates to Karthik and Ananthanarayana's TRUST framework in the following ways.

- Similarities include the following.
  - Both use the formalisms of an ontology and rules with the aim of supporting trust-related decisions.
  - Both use the notion of the subject as trustor and the object as potential trustee.
  - Both use provenance of information in the evaluation of trustworthiness.
- The following are the main differences.
  - While the $\mathcal{TE}$ framework imports other ontologies to improve interoperability, the Karthik and Ananthanarayana TRUST framework does not.
  - While the $\mathcal{TE}$ framework gives a truth-functional interpretation to the outcome of a trustworthiness evaluation, the TRUST framework gives a trust score (a numerical value such as 0.3). The $\mathcal{TE}$ framework does not use numerical values, because we argued in Section 3.5.3.2 that it is not useful for trust.
  - While the $\mathcal{TE}$ framework makes its evaluation rules publicly available through the publication of a rulebook and the corresponding queries, the rules used by the TRUST framework are not available.
  - The TRUST framework focuses on decisions related to a pervasive sensor-driven network, while the $\mathcal{TE}$ framework addresses the broader setting of a potential trustor and a potential trustee.
  - The $\mathcal{TE}$ framework includes an automated mechanism to create instance data. How to generate instance data for the TRUST framework is not addressed.

15.3.6.3 Karuna et al. – the UTPO ontology

Karuna et al. [198] describe a trust model for on-line health information systems. The model consists of a taxonomy of trust factors which is implemented as the User's Trust Profile Ontology (UTPO) in OWL. The taxonomy of trust factors and validate it through a user survey based on nine responses. The $\mathcal{TE}$ framework relates to the UTPO ontology in the following ways.

- Similarities include the following.
  - Both use the formalisms of an ontology with the aim of supporting trust-related decisions.
  - Both implementations make use of OWL DL.
- The following are the main differences.
  - The focus of the UTPO ontology is on-line healthcare systems, while the $\mathcal{TE}$ framework addresses the broader setting of a potential trustor and a potential trustee.
  - While the $\mathcal{TE}$ framework imports other ontologies to improve interoperability, the UTPO ontology does not.
  - The UTPO ontology is, as its name implies, limited to an ontology. There is no discussion of how to instantiate the ontology for practical use cases, or how to use the trust factors it proposes.
  - The UTPO ontology is intended to be used as the basis for a recommender system with numerical values, while the $\mathcal{TE}$ framework gives a truth-functional interpretation to the outcome of a trustworthiness evaluation.
  - The $\mathcal{TE}$ framework includes an automated mechanism to create instance data. How to generate instance data for an instantiation of the UTPO ontology is not addressed.

15.3.6.4 Kravari and Bassiliades – the ORDAIN ontology

Kravari and Bassiliades [205] propose ORDAIN as a general-purpose ontology for trust management in the Internet of Things. The $\mathcal{TE}$ framework relates to ORDAIN in the following ways.

- Similarities include the following.
  - Both use the formalisms of an ontology with the aim of supporting trust-related decisions.
  - Both use OWL DL for their implementation.

- The following are the main differences.
  - While the $\mathcal{TE}$ framework imports other ontologies to improve interoperability, the ORDAIN ontology does not.
  - The ORDAIN ontology focuses on reputation, which is assumed to be the prime factor in the establishment and maintenance of trust between parties. The $\mathcal{TE}$ framework focuses on evaluation of trustworthiness.
  - While the $\mathcal{TE}$ framework gives a truth-functional interpretation to the outcome of a trustworthiness evaluation, ORDAIN is based on data aggregation and confidence level calculations. The $\mathcal{TE}$ framework does not use numerical values, because we argued in Section 3.5.3.2 that it is not useful for trust.
  - While the $\mathcal{TE}$ framework makes its evaluation rules publicly available through the publication of a rulebook and the corresponding queries. The calculation of the reputation score is not addressed in ORDAIN.
  - The $\mathcal{TE}$ framework includes an automated mechanism to create instance data. How to generate instance data according to the ORDAIN ontology is not addressed.

15.3.6.5 Oltramari and Cho – the ComTrustO framework

Oltramari and Cho [261] propose ComTrustO, a composite trust-based ontology framework fusion, modelled in OWL. The $\mathcal{TE}$ framework relates to ComTrustO in the following ways.

- Similarities include the following.
  - Both use the formalisms of an ontology with the aim of supporting trust-related decisions.
  - Both import other ontologies to improve interoperability.
  - Both address the setting of a potential trustor and a potential trustee.
  - Both address trust as multidimensional. ComTrustO is a composite ontology of four layers (communication trust, information trust, social trust and cognitive trust). In the $\mathcal{TE}$ framework this is addressed by the integrated requirements and the selection of data points in multiple dimensions.
- The following are the main differences.
  - ComTrustO is, as implied by its name, an ontology. How to use the ontology (which typically involves an instantiation of individuals of the classes defined by the ontology), or how to support decision-making (e.g. by rules), is envisaged as future

research. Oltramari and Cho [261] state that they plan to investigate the applicability of real data sets. The $\mathcal{TE}$ framework includes an ontology and a set of reasoning rules. Furthermore, the data import and transformation mechanism has been instantiated to create instance data on the basis of real data sets.

15.3.6.6 Sel – the Trust Claim Interpretation model

Sel [296] proposed the Trust Claim Interpretation (TCI) model. It is based on a combination of newly defined classes and existing vocabularies from W3C. The $\mathcal{TE}$ framework relates to the TCI model in the following ways.

- Similarities include the following.
  - Both address the setting of a potential trustor and a potential trustee.
  - Both use the formalisms of an ontology and rules with the aim of supporting trust-related decisions.
  - Both import other ontologies to improve interoperability.
- The following are the main differences.
  - In the TCI model, unlike the $\mathcal{TE}$ framework, the creation of classes is not based on an analysis of requirements.
  - The TCI model involves significant manual effort for the manual translation of observations about entities into instances of a TCI class. The $\mathcal{TE}$ framework has automated this translation using XSL. Also, the operation of the $\mathcal{TE}$ framework has been demonstrated using real-world data converted into FOL via data import and transformation mechanisms.
  - The TCI model includes only a limited set of example rules. The $\mathcal{TE}$ framework includes the concept of a rulebook consisting of pre-specified rules. Furthermore the $\mathcal{TE}$ framework allows the specification of a trustworthiness evaluation policy, based on the distinction between mandatory and discretionary rules.

15.3.6.7 Sullivan et al. – the Trust-term ontology

As described in Section 3.5.2.1, Sullivan et al. [307] define security requirements, metrics and trust terms in the form of a Trust-term ontology. The $\mathcal{TE}$ framework relates to the Trust-term ontology in the following way.

- Similarities include the following.

  - Both use the formalisms of an ontology.
  - Both attribute importance to transparency and identification.
  - Both address the setting of a potential trustor and a potential trustee.

- The following are the main differences.

  - The Trust-term ontology does not make use of other existing ontologies to improve interoperability. Rather it aims to refine the terminology related to security and trust. The ontology of the $\mathcal{TE}$ framework builds on multiple existing ontologies, as described in Section 11.2.3.
  - The Trust-term ontology uses the property 'fosters' to link anonymity to trust. The ontology of the $\mathcal{TE}$ framework does not cover anonymity, because anonymity was not identified as a necessary characteristic for the context of interest.
  - The Trust-term ontology explicitly defines accountability, which the property 'facilitates' links to responsibility. The ontology of the $\mathcal{TE}$ framework addresses this implicitly, through legal attestations.
  - The Trust-term ontology does not address instance data, as it limits its scope to terminology. The $\mathcal{TE}$ framework encompasses instance data to demonstrate how to reason with the concepts defined in the ontology.

15.3.7 Summary of the comparison

The $\mathcal{TE}$ framework has the following characteristics that go beyond the prior art.

When compared to the use of trust in trusted third parties, the $\mathcal{TE}$ framework is more precise in terms of semantics regarding the meaning of trustworthiness because it allows a potential trustor to select data points that represent information with a specific meaning regarding a potential trustee, from a qualified and distributed set of data sources.

When compared to the use of trust in the Web of Trust, the $\mathcal{TE}$ framework allows:

- a more granular specification of the interrelationships between participants through its use of attestations, and
- the chaining of relationships, which makes it possible to evaluate chains of edges such as those created by the relationships between accreditation bodies, conformity assessment bodies and evidence service providers.

When compared with trust-related ontologies, the $\mathcal{TE}$ framework has the following additional characteristics.

- It includes evaluation criteria for data sources, as well as methods to automatically create instance data about the potential trustees and their context from selected data sources.
- It builds on existing W3C ontologies to enable interoperability.
- It has a formal data model that addresses the context (accreditation, conformity, legal qualification) of the relationship between a potential trustor and a potential trustee.
- It includes a basic rulebook in FOL, and allows implementation of specific rulebooks on the basis of the data model and this basic rulebook.

15.4 Summary

This chapter presented experimental results of the partial implementation of the $\mathcal{TE}$ framework. Using a home-office Internet connection and a regular laptop, all individual operations (downloads, transformations, data base load, queries) could be performed in less than or approximately one second.

A comparison against existing frameworks was also given, covering the well-known trust concepts such as those from Marsh and from Bacharach and Gambetta, the PKI and WOT models, and the most relevant trust-related ontologies.

Chapter 16

Summary and conclusions

This chapter concludes the thesis by providing a summary and a review of the work performed. This leads naturally to a detailed assessment of the validation of the trustworthiness evaluation framework proposed in the thesis. Areas for further research are also described.

16.1 Introduction

The thesis proposed a novel approach to improving interpretations of claims of trustworthiness. It was argued that one should not 'trust' but rather take an informed decision on the basis of evidence and reasoning. Data points that represent evidence from multiple data sources can be combined and logically reasoned about.

This chapter presents the conclusions of the thesis and describes areas for further research. It is structured as follows.

- Section 16.2 provides a summary of the $\mathcal{TE}$ framework and the partial implementation developed to validate it.
- Section 16.3 presents a review of the main hypothesis of the thesis, and gives answers to the research questions on the basis of the work performed.
- Section 16.4 proposes areas for future work.
- Section 16.5 provides a summary of the chapter.

16.2 The $\mathcal{TE}$ framework

The objective of the $\mathcal{TE}$ framework is to allow a potential trustor to evaluate the trustworthiness of a potential trustee. This evaluation is based on verifying whether a set of rules is satisfied

by particular instance data. The framework contains four classes of components: a data model, rulebooks, trustworthiness evaluation functions and methods to create instance data about the potential trustees and their context. To demonstrate the practical feasibility of the proposed solution, a partial implementation was developed.

16.2.1 Requirements

The requirements for the framework were given in Chapter 5, and were developed on the basis of a literature review and the requirements developed in the Horizon2020 FutureTrust project[1] work packages [229], [230]. Requirements from these sources were combined into the following set of integrated requirements.

- IR1 Semantic definition of trustworthiness: *As a participant in an electronic ecosystem I can understand the meaning of trustworthiness of participants I plan to engage with, so that I can make an informed decision on whom to interact with.*
- IR2 Transparency: *As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate trustworthiness of other participants, I can access all information (including inputs used and operations performed) of this function in a transparent way, so that I can understand the factors that contribute to trustworthiness and their mapping on evidence such as qualifications of entities.*
- IR3 Linked and unique identity: *As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate the trustworthiness of other participants, I can rely on this function combining all information about participants available within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation is based on all information known about the evaluated participant.*
- IR4 Competently acting in role *As a participant in an electronic ecosystem I have access to and I can demonstrate that I accept the definitions of roles, the qualifications that are required per role, and how these qualifications are demonstrated by participants, so that I can verify these arguments are suitable to support the reliance I want to take on the outcome of the reasoning.*
- IR5 Governance, security and controls: *As a participant in an electronic ecosystem I can understand the governance, security safeguards and controls that are in place within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation took into consideration that the ecosystem meets good practices regarding these topics.*

[1] http://www.futuretrust.eu

- IR6 Policy choices: *As a possible participant in an electronic interaction I can determine the information and the reasoning justifying that a participant is qualified as trustworthy, so that I can verify that information and reasoning are compatible with the way I want to rely on the reasoning's outcome.*

- IR7 Obtaining credible data: *As a participant in an electronic ecosystem I can understand the origin and the type of data that is used in the evaluation of trustworthiness of participants, so that I can claim the outcome of the trustworthiness evaluation is based on credible data.*

16.2.2 Framework participants

The framework positions participants within an ecosystem, divided into three planes, described in Chapter 6. Participants may invoke services provided by participants from any plane. The enabler plane consists of the participants whose role is to enable trustworthiness, and also contains the rulebooks and the trustworthiness evaluation functions which are available to all participants. The roles in this plane are as follows.

- An *authentic source* holds a mandate to register and validate information about entities and makes this information available. The mandate can be a document that has legal validity because it is published in an official journal or because it is accepted to be binding through a contract or membership agreement.

- An *endorser* expresses its publicly visible approval for a rulebook through its endorsement, and makes information on responsibility, accountability, and authority to implement security governance available either itself or endorses information made available by others.

- An *enforcer* is an entity with power to enforce consequences among participants. An enforcer acts as arbiter or judge and provides the possibility for redress. Enforcement is outside the proposed system, but information about whether enforcement is available can be captured and reasoned about.

- An *accreditation body* is an entity that performs accreditation, i.e. the independent evaluation of conformity assessment bodies against recognised criteria for their impartiality and competence. An accreditation body accredits participants in the role of a conformity assessment body.

- A *conformity assessment body* assesses the conformity of participants and their services against relevant criteria, and provides assurances of conformity in the form of attestations.

The trustworthiness provision plane involves participants that provide trustworthiness services. The principal roles in this plane are as follows.

- An *evidence service provider* creates information that serves as evidence. It includes traditional Trust Service Providers such as Certification Authorities, Identity Providers, Attribute Providers, (Remote) Signature Services, Time Stamp Services, etc.
- A claim status service provider provides status information regarding claims, e.g. verifying a response to an authentication request, or verifying an electronic commitment or signature.
- A trustworthiness monitor is a participant that monitors and attests the services from evidence service providers and claim status service providers.

The functional plane consists of participants that act in the role functional service providers, that offer business services, and functional service consumers, that interact with the former.

16.2.3 Data model

Predicates are used to model the data points that are used for trustworthiness evaluation. The purpose of the predicates is to represent things from the real world, so that they can be reasoned with. 15 predicates were specified in Chapter 7, of which a selection is listed below. S always refers to the Subject.

- *Actor*(X), an entity without any attestation
- *Attestation*(a_{id}, T), where a_{id} = the identity of the issuer of the attestation and triple T =$\{S, A, V\}$ where A refers to Attribute and V to Value
- *Participant*(X)
- *Base role* specified as *Attestation*(a_{id}, (S, *roleTypeBase,* V)) where V refers to an instance of a role type
- *Accreditation*(a_{id}, (S, *accreditedFor,* N) where N refers to Norm
- *Conformance*(a_{id}, (S, *doesConformTo,* N) where N refers to Norm
- *LegalQualification*(a_{id}, (S, *legalQual,* L) where L refers to a legal qualification such as a law, regulation, act, or decree

16.2.4 Rulebooks

The concept of a rulebook was specified in Chapter 8. The purpose of a rulebook is to formally capture an understanding of what trustworthiness means in a particular context, where this understanding is captured in the form of constraints. The rules were specified in FOL, using the predicates defined in the data model.

A rulebook contains a mandatory and a discretionary part. The mandatory constraints verify the basis for relevant execution of the discretionary rules. The latter can be selected by a potential trustor to configure a policy for trustworthiness evaluation.

16.2.5 Trustworthiness evaluation

16.2.5.1 The function $twseval_{AE}$

The trustworthiness evaluation function $twseval_{AE}$ is used to verify that an ecosystem is trustworthy. The function takes the form

$$twseval_{AE}(R_{id}, \{DiscretionaryRules\}, InstanceData)$$

where

- R_{id} identifies the applicable rulebook,
- $\{DiscretionaryRules\}$ denotes the set of discretionary rules selected by the trustor, and
- *InstanceData* identifies the instance data that is to be used.

Execution of the function includes verification of the mandatory rules of the selected rulebook. The function returns *true* when all of the evaluated rules return *true*. *True* means that the evaluated ecosystem meets the constraints specified in the rules, which is an indication of trustworthiness. The function returns *false* when at least one of the evaluated rules returns *false*. *False* means that the evaluated ecosystem does not meet the constraints specified in the rules, which is an indication of a possible lack of trustworthiness.

16.2.5.2 The function $twseval_{AP}$

The trustworthiness evaluation function $twseval_{AP}$ is used to verify that a participant is trustworthy. The function takes the form

$$twseval_{AP}(RBK_{id}, P_1, target\_base\_role\_X, \{DiscretionaryRules\}, InstanceData, \{Norms\})$$

where

- RBK_{id} denotes the identification of the applicable rulebook,
- X denotes the identification of the potential trustee,
- *target_base_role_X* denotes the target base role of X, i.e. the role the trustor would expect the trustee X to act in,
- *{DiscretionaryRules}* stand for the set of discretionary rules selected by the trustor, which allows to configure a trustworthiness evaluation policy, and
- *InstanceData* denotes the reference to the instance data that is to be used,
- {*Norms*} denotes the set of discretionary norms (i.e. legal acts and technical standards) the trustee is expected to provide attestations of conformity assessment to.

Execution of the function includes verification of the mandatory rules of the selected rulebook. The function returns *true* when all of the evaluated rules return *true*. *True* means that the evaluated participant meets the constraints specified in the rules, which is an indication of trustworthiness. The function returns *false* when at least one of the evaluated rules returns *false*. *False* means that the evaluated participant does not meet the constraints specified in the rules, which is an indication of a possible lack of trustworthiness.

16.2.6 Implementation

16.2.6.1 Technical set-up

The framework was implemented in an architecture that is composed of a front-end and back-end layer. The front-end layer contains the $\mathcal{TE}$ data model[2] created using Protégé [250], transformation programs[3] that download information from the data sources and transform it according to the $\mathcal{TE}$ data model, and SPARQL queries whose answers allow to verify the satisfaction of the rules. The back-end layer stores the downloaded information as instance data in an Ontotext GraphDB database[4].

16.2.6.2 Instance data

The creation of instance data was addressed in Chapter 12. For the trustworthiness evaluation to be based on credible data, such data must come from authoritative sources that allow access to data that corresponds to one or more predicates. This lead to the following selection criteria. The data source must offer data that is specified in the data model, it must be authoritative

[2] `http://www.marcsel.eu/onto/te/te-data-model.owl`
[3] Developed in a combination of Java and Extensible Stylesheet Language Transformations [377] (XSLTs).
[4] https://graphdb.ontotext.com/

for this data, it must include a description of its meaning, and the data must be available in a machine readable format.

There are a number of data sources capable of providing data corresponding to one or more predicates. The current implementation limits itself to data sources in the public domain. On the basis of the selection criteria, the European Trusted Lists[5] and the Linked Open Data source FactForge[6] were selected as data sources for information about companies. Data sources were also selected for information about accreditation, conformity assessment and legal attestation. Using the same selection criteria, a FOAF file from Elsevier's Mendeley Data Search (described by Petrovic and Fujita [273]) and one of the author's X.509 certificates, produced by the Belgian national identity register, were used as data sources about natural persons. The selected data was downloaded and transformed into triples that could be loaded in the graph database. Provenance information was added to indicate the original data source of the information in the database.

16.2.6.3 Rulebook implementation

A specific rulebook, inspired by the eIDAS Regulation [103] and meeting the requirements defined in Chapter 5, was described in Chapter 13. Requirement IR1 is addressed by formulating the rules in FOL using a taxonomy of data points that have a truth-functional interpretation. While FOL adds value through its truth-functional interpretation, the implementation refines this by using the Organization (ORG) ontology [376] and the Provenance (PROV-O) ontology [357]. This improves interpretation because the ontologies are written in OWL, which allows expression of fine-grained constraints and provides an interpretation in natural language. Rules were defined to address requirements IR2, IR3, IR4 and IR5 in the following ways.

- IR2 is addressed by making the data model, the rules and the trustworthiness evaluation functions publicly available, by using instance data from publicly available sources, and by the specification of rules. Mandatory rules specify requirements on existence and identification of the rulebook and naming of participants. Ten discretionary rules specify requirements on the existence of participants in specific roles.

- IR3 is addressed by defining a mandatory rule regarding the uniqueness of identity. Discretionary rules specify requirements on identity attestation regarding self-attestation, increasingly stringent third-party attestation and legal attestation of identity.

- IR4 is addressed by defining a mandatory rule on role attestation regarding self-attestation, and discretionary rules specify increasingly stringent attestation requirements for the different roles, including the legal attestation of roles.

[5] `https://ec.europa.eu/tools/lotl/eu-lotl.xml`
[6] `http://factforge.net`

- IR5 is addressed by defining discretionary rules that cover disclosure and segregation of duty.

IR6 is addressed by keeping the number of mandatory rules minimal, and allowing the potential trustor to select discretionary rules that correspond best to its policy. IR7 is addressed by defining selection criteria for data sources from where the instance data will be generated.

16.2.6.4 Evaluation of trustworthiness

An evaluation of an entity as a potential trustee involves the following steps. The trustor must connect to the database that holds the instance data, select the discretionary rules of its choice and execute the queries that correspond to the mandatory and selected rules. The query results allow satisfaction of the rules to be verified.

16.3 Review

16.3.1 Review of hypothesis

Section 1.2.2 contains the following hypothesis: 'Where machine processable information about actors is available, it is desirable and possible to automate reasoning about the properties of these actors to support trust-related decision making based on formal semantics.'

Evidence was identified that supports this hypothesis. As shown in Part II, logical specifications can be formalised that describe properties of actors relevant to trust-related decision making, and the evaluation of trustworthiness can be modelled as constraint satisfaction. Part III demonstrated:

- that authentic data sources containing the required information in machine readable format are available;
- how the logical specifications, elaborated in Part II, can be implemented with formal semantics in OWL and in a graph database, and how this allows automated reasoning about the properties of actors to support trust-related decision making.

16.3.2 Review of research questions

The following answers to the research questions that were posed in Section 1.2.3 derive from the work described.

16.3.2.1 How can we semantically define trustworthiness?

As trust is a social concept, we did not attempt to describe it in the context of the electronic society. However, we demonstrated in Part II that a meaningful description of trustworthiness can be given using a data model, rulebooks and a specification of trustworthiness evaluation. These were developed on the basis of a set of requirements that were established in Chapter 5. Requirements IR1 *Semantic definition of trustworthiness* and IR2 *Transparency* contributed specifically to the elaboration of a meaningful description.

16.3.2.2 How can we reason about trustworthiness?

It was demonstrated that formal logic, aided by transparency and credible input data can assist in automating claims of trustworthiness. Claims of trustworthiness can be evaluated on the basis of a policy. Compliance to the policy can be demonstrated by the execution of queries over the graph database. Chapter 8, and particularly Section 8.2, describe how constraints on data points that represent relationships or attributes can be formalised as rules in FOL. Chapter 13 demonstrates how these rules can be implemented in OWL. Chapter 14 provides a description of how the results of the execution of these rules can be interpreted.

16.3.2.3 On what can reasoning to qualify an entity as trustworthy be based?

A trustworthy ecosystem was proposed in Chapter 6, and on the basis of the roles given there, the required information was identified and a corresponding data model was defined in Chapter 7. Requirements IR4 *Competently acting in role* and IR5 *Governance and controls* contributed to the identification of the required information to support the proposed reasoning.

16.3.2.4 Obtaining information for use in reasoning

The fourth research question was formulated as *How can we obtain information for use in supporting such reasoning about 'real world' entities?*

Selection criteria for the required information artefacts were specified in Chapter 12, and data sources were identified. For relevant data sources, transformation programs were developed that converted information in XML format to OWL XML/RDF format. Where the information was not available in machine-readable format, manual conversion was done on the basis of publishes PDF documents. Such manual conversions obviously do not scale. Requirement IR7 *Obtaining credible data* contributed to the development of the data import and transformation method.

16.4 Areas for future research

16.4.1 Identity issues

As described in Section 7.5, the $\mathcal{TE}$ framework is built on the assumption that a unique linkable identity can be implemented. Whether this is both feasible and desirable is an open question. Recent work in this area includes the following.

- The Solid[7] initiative, described by Werbrouck et al. [383], has developed a set of conventions and tools for building decentralized social applications based on Linked Data principles. Solid relies on existing W3C standards and protocols. These include RDF for resource description, Web Identity and Discovery (WebID) to provide universal usernames/IDs for Solid apps, and to refer to agents (people, organizations, devices), and the FOAF vocabulary. The objective is to give users direct control over their identity attributes. For this purpose, such attributes are stored in a so-called Solid pod. Before an application has access to an attribute, the user needs to grant permission for this. As opposed to the current model used by big tech companies, this gives the control over identity and other attributes back to the user.

- Project SEAL[8], described by Aragó-Monzonís et al. [7], has identity reconciliation as its prime focus. The envisaged functionality of SEAL is to act as a trusted authority to issue information about the relationship between different identities and data sets.

- Verheul et al. [329] proposed polymorphic encryption and pseudonymisation as a novel approach for the management of personal data and of pseudonymous authentication. The proposed scheme is based on the homomorphic properties of the ElGamal algorithm [84]. For an overview refer to Appendix J.2.1. The key idea of polymorphic encryption is that directly after generation, data can be encrypted in a 'polymorphic' manner and stored as such. There is no need to decide a priori who will be allowed to see the data. This decision will be made on the basis of a policy, in which the data subject should play a key role. The encrypted data can be tweaked to make it decryptable by a specific party. This tweaking can be done in a blind manner, by a trusted party who knows how and for whom to tweak the ciphertext. The proposed polymorphic pseudonymisation infrastructure guarantees that each individual will automatically have different pseudonyms for different parties and can only be de-pseudonymised by participants who know the original identity.

Future work on the $\mathcal{TE}$ framework could investigate whether a subset of identity attributes would be sufficient for trustworthiness evaluation. Additionally, the extend to which privacy

[7] `https://solidproject.org/`
[8] `https://project-seal.eu/`

enhancing techniques could aid in reducing the need for a single unique linked identity, or could replace it by another approach, are interesting possible directions for further work.

16.4.2 Further semantic refinement

As described in Chapter 11 and in Appendix D, the framework implementation makes use of a selection of existing ontologies.

- Additional ontologies could be analysed for identification of additional data points that further improve trustworthiness evaluation. Candidate ontologies include the following.
  - The W3C Registered Organization Vocabulary[9] (RegORG) is a profile of the Organization Ontology intended for describing organisations that have gained legal entity status through a formal registration process, typically in a national or regional register. A Registered Organization is a sub class of the Organization Ontology's Formal Organization. RegORG includes three sub properties of ORG's classification property covering status, activity and type. It uses the identifier issued by the relevant registration authority that confers legal status.
  - MetaLex and Legal Knowledge Interchange Format (LKIF), as described by Boer et al. [35], are relevant ontologies. MetaLex is an interchange format intended to impose a standardised view on legal documents for the purposes of information exchange and interoperability in the context of software development. LKIF was designed with the goal of becoming a standard for representing and interchanging policy, legislation and cases, including their justificatory arguments, in the legal domain.
- The use of ontologies that cover the legal domain, and additional data points that address legal information could allow expression of legal effects such as presumption of validity, exemption from the burden of proof and assumption of legal compliance as components of the evaluation of trustworthiness.
- Selective classes of the FIBO ontologies, described in Section D.2.3, are currently used in the implementation. As these ontologies contain a rich set of data points, their further potential could be studied.

Future research could investigate whether the use of these ontologies can contribute to more refined semantics of trustworthiness.

[9] `https://www.w3.org/TR/vocab-regorg/`

16.4.3 Data model extensions

The proposed data model provides a foundation for trustworthiness evaluation. Section 6.3 specified two types of roles: base roles and situational roles. The current data model and the corresponding trustworthiness evaluation are limited to base roles. A situational role indicates a specific participant role in a situation. Examples of situations include an interactive session, an information transfer, and the storage/retrieval of information. Situational roles are, as indicated by their name, bound to a specific situation. The use of situational roles is a topic for future research.

16.4.4 Rulebook extensions

The proposed rulebook can serve as a basis for trustworthiness evaluation, but it can be extended. Future research topics in this area include the following.

- Governance aspects could be further incorporated. The current specification is limited to governance of information security. There are several other areas of governance within an organisation, such as governance of information technology, and organisational governance. How governance of such areas could contribute to trustworthiness is a possible future research topic, potentially covering both the operation of the governance processes and the outcome of these processes.
- Security safeguards could be further incorporated. For example rules on the use of trustworthy hardware and/or software could be envisaged. Such rules could be based on conformity assessment.
- The dependency of a participant on another participant, such as created through ownership, may influence trustworthiness in specific situations. How independence (or the lack thereof) of participants could contribute to trustworthiness is a possible topic for future research.
- How to create rulebooks for a consensus-governed society rather than for a law-governed society could usefully be investigated. This could include the role of membership organisations such as the Kantara Initiative[10] as accreditation body and as publisher of a trust list. In such a consensus-governed society the participants must be attested by other participants using a consensus scheme. Many consensus-based schemes that are based on blockchain technology are emerging.

[10] `https://kantarainitiative.org/`

16.4.5 Evaluation-related

16.4.5.1 Use of logic

Regarding the use of logic in the evaluation function, the following topics are candidates for further research.

- The evaluation functions makes use of instance data which contains information about a specific set of entities. The current system is limited to instance data that can be used as positive evidence, i.e. evidence which would allow a target role to be judged untrustworthy is not taken into account. The study of negative evidence is a possible topic for future research.
- The thesis makes use of FOL to describe the proposed rulebook. Rules related to separation of duty could benefit from being specified algebraically, e.g. as proposed by Li [218]. Such an algebra supports the combination of quantitative requirements (such as that k different users must be involved in a sensitive task), with minimal qualification requirements for these users. How such an algebra could contribute to trustworthiness is an interesting topic for further research.
- The partial implementation relies on SPARQL queries to evaluate trustworthiness. This evaluation (or parts thereof) could alternatively be based on additional classes and inference, as calculated by the inference engine. The potential benefits of using a more inference-based approach could be further investigated.

16.4.5.2 Evaluation policies

The proposed evaluation policy mechanism, where a potential trustor selects the rules most relevant to its situation, is described in Chapter 14.1. This could helpfully be extended to address to address the third underlying problem of trust, as described in Section 15.3.3.2. A brief description how this might be done is provided below.

A matrix representation with the dimensions Source ('attested by') and Evaluator ('evaluated by') could be used to model the relations between self and others. Such a trustworthiness evaluation matrix is illustrated in Figure 16.1. The trustworthiness matrix represents two principles that are relevant to trustworthiness evaluation.

- The first principle is the selection by the potential trustor of the source of information used during trustworthiness evaluation. This source must be known. To make this assumption reasonable, it is required that there is a reliable way to determine the information sources used and to identify the derived information as such. The x-axis indicates the source of the data points. This is addressed by participants and attestations as follows.

  - 'Trustee self' (or 'self-claimed') corresponds to a participant that attests (claims) its own trustworthiness ('trust me'). In the non-electronic world this corresponds to what is commonly known as 'unsworn declarations' where a signer of a document declares that the signature is executed under penalty of perjury and no other individual is involved[11].
  - 'Unqualified other', which corresponds to a participant who claims trustworthiness about another participant ('trust them because I tell you') without having a legal qualification to do so. While the claimant may have a (hopefully positive) reputation that is publicly known, or other qualifications that are not based on a legal foundation, the claimant does not have one or more relevant legal qualifications.
  - 'Qualified other', which corresponds to a participant that claims trustworthiness about another participant ('trust them because I tell you and I am legally qualified in this'). The claimant does have particular legal qualifications such as accreditations to make the claim trustworthy.

- The second principle is the choice by the potential trustor of the executor of the trustworthiness evaluation function. To make this assumption reasonable, it is required that there is a reliable way to determine the executor and to identify the derived outcome. The y-axis indicates the performer of the evaluation, which is one of the following.

  - 'Trustor self', which corresponds to a participant that executes its own trustworthiness evaluation ('rely on self'). Given the complexity of today's interactions in electronic ecosystems and given that the knowledge and capabilities of a participant are always limited, higher trustworthiness can be obtained from combining one's own knowledge and capabilities with those from others.
  - 'Unqualified other', which corresponds to a participant who relies on a trustworthiness evaluation performed by another participant ('trust them because I tell you') without that participant having a legal qualification to do so. While the claimant may have a (hopefully positive) reputation that is publicly known, or other qualifications that are not based on a legal foundation, it does not have one or more relevant legal qualifications.
  - 'Qualified other', which corresponds to a participant that relies on a trustworthiness evaluation performed by another participant ('trust them because I tell you and I am legally qualified in this'). The claimant has particular legal qualifications such as accreditations to make the claim trustworthy.

[11] In an unsworn declaration, the contents and signer can vary widely. The contents can be about oneself or another, and the signer can be anyone, with or without qualifications of any type. The 'trustee self' case can only be compared to an unsworn declaration whose content provides information about the signer.

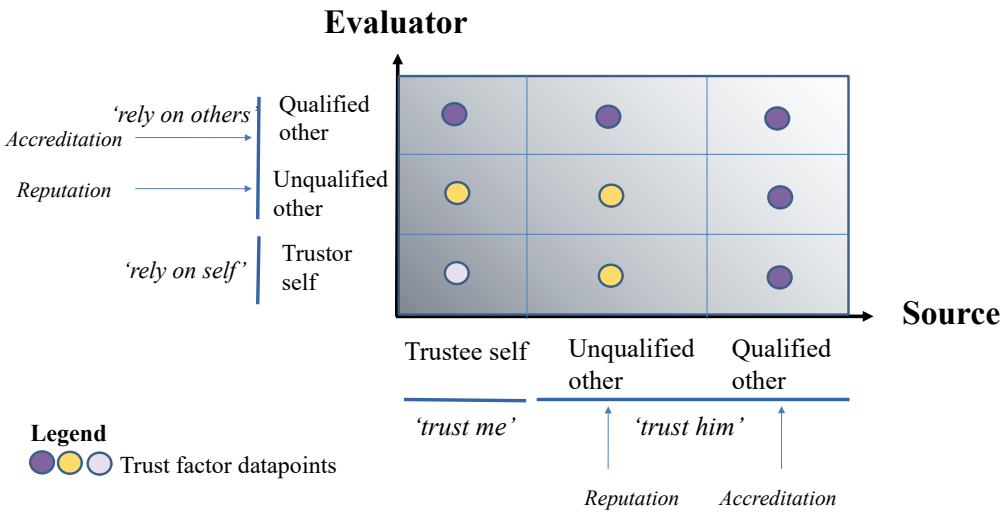

Figure 16.1: Trustworthiness evaluation matrix

It is assumed that the distinction between self and other can easily be made. However, the distinction between unqualified and qualified other needs to be specified. It is assumed here that the $\mathcal{TE}$ framework is used in a law-governed society and this distinction is based on whether or not the qualification has a legal basis. Other approaches are possible. The emerging self-sovereign models for deciding what information to accept as truth are based on consensus protocols. Rulebooks could be created for such a consensus-governed society where the participants must be attested by other participants using a consensus scheme. This is a possible topic for further research.

The matrix supports multiple trustworthiness evaluation policies. Such a policy can be described by specifying the included matrix quadrants. This would allow the following policy examples.

- A trustor may decide to only rely on itself for evaluation, and to make use of data sources provided by qualified others.
- A trustor may decide to only rely on itself for evaluation, but to make use of all of the categories of data sources (trustee self, unqualified other, qualified other).
- A trustor may decide to rely only on a qualified other to perform the evaluation, and to use data that is provided by qualified others.

16.4.5.3 Attestation of trustworthy execution

A situation can be envisaged where the potential trustor does not have access to a trustworthiness evaluation function under its control. This might be due to a lack of resources or device constraints, or because the required instance data is not available. In such a situation it would be necessary to rely on another party to execute the function and return the results. The choice by the potential trustor of the executor of the trustworthiness evaluation function could be supported by the qualifications of the execution environment. Huh and Martin [160] proposed the idea of a 'configuration resolver' for trustworthy distributed systems. A configuration resolver maintains an up-to-date whitelist and performs attestation on the user's behalf, ensuring that the tasks to be executed are dispatched to only those considered trustworthy. This aims to provide a more usable attestation service for large-scale distributed systems. How this could be formulated as $\mathcal{TE}$ framework attestations and integrated in a rulebook is a possible topic for future research.

16.4.6 Data import and transformation

16.4.6.1 On-line access to data

The implementation presented above involves the use of a data import function. An alternative implementation using an on-line access function could be investigated. Such an approach could be beneficial for the freshness of the information that is obtained.

16.4.6.2 Use of more trusted list data

For the specific rulebook that was proposed in Chapter 13, the participant assertions in the graph database include information derived from European trusted lists. However, the implementation does not use the service status indication[12]. This information distinguishes between the statuses of granted, undersupervision and withdrawn, and could be imported, transformed into assertions and evaluated.

16.4.6.3 Additional data sources

The use of additional data sources, which continue to emerge, could usefully be investigated, e.g. as follows.

- The Governments of British Columbia, Ontario and Canada recently initiated an on-line registry[13] of what they refer to as 'verifiable organisations'. It offers its blockchain-based

[12] <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted | undersupervision | withdrawn</ServiceStatus>

[13] `https://orgbook.gov.bc.ca/en/home`

information through a public API[14]. Since the information is created by officially recognised authentic sources, this offers a new mechanism for on-line verification of participant information.

- In Europe, the following data sources are candidates for further analysis and potential implementation in the trustworthiness evaluation function.
  - As a result of the amended Transparency Directive in 2013, companies listed on EU regulated markets are required to prepare their annual financial reports in a European Single Electronic Format (ESEF). All annual financial reports must be prepared in XHTML format, and where the reports contain IFRS consolidated financial statements they must be labelled with XBRL (eXtensible Business Reporting Language).
  - The list of national accreditation bodies and the CABs was recently consolidated and made publicly available[15].
  - As described in Section 4.3.1.3, the National Archives publish all UK legislation on behalf of HM Government, and 'The Gazette' is an official journal of record which consists largely of statutory notices. Both are available in machine-readable RDF format.
  - EU legislation is published by the Publication Office[16]. The information is made available in various ways, including an API, a SPARQL endpoint and an RSS feed.

16.4.6.4 Data transformation

The possible further automation of XSL-based transformations using technology specifically developed for the creation of graphs on the basis of existing data could be investigated. Examples include the RMLMapper[17] which relies on declarative rules that define how the knowledge graphs are generated.

16.4.7 Further ideas

16.4.7.1 Ex-post evaluation

As described in Section 6.7, a potential trustor can use the trustworthiness provision and evaluation services before an interaction (ex-ante), during an interaction or after an interaction (ex-post). Only the first of these (ex-ante) was analysed. The other two types of evaluation are left

[14] https://vonx.io/

[15] https://ec.europa.eu/futurium/en/system/files/ged/list_of_eidas_accredited_cabs-2019-08-23.pdf

[16] https://op.europa.eu/en/web/web-tools/

[17] https://rml.io/

for future work. For example, the ex-post use of trustworthiness evaluation may be particularly relevant because it can provide information that is complementary to the verification of an electronic signature.

16.5 Summary

This chapter presented the main conclusions of the thesis and described areas for further research. A review of the hypothesis of the thesis was presented, and answers to the research questions were given on the basis of the work performed. Finally, areas for further research were proposed.

Bibliography

[1] I. M. Abbadi and A. Martin. Trust in the cloud. *Information security technical report*, 16(3-4):108–114, 2011.

[2] A. Abdul-Rahman. The PGP trust model. *EDI-Forum: the Journal of Electronic Commerce*, 10(3):27–31, 1997.

[3] H. Akkermans and J. Gordijn. Ontology engineering, scientific method and the research agenda. In S. Staab and V. Svátek, editors, *Managing Knowledge in a World of Networks, 15th International Conference, EKAW 2006, Podebrady, Czech Republic, October 2-6, 2006, Proceedings*, volume 4248 of *Lecture Notes in Computer Science*, pages 112–125. Springer, 2006.

[4] A. Aldini. A calculus for trust and reputation systems. In J. Zhou, N. Gal-Oz, J. Zhang, and E. Gudes, editors, *Trust Management VIII — 8th IFIP WG 11.11 International Conference, IFIPTM 2014, Singapore, July 7-10, 2014. Proceedings*, volume 430 of *IFIP Advances in Information and Communication Technology*, pages 173–188. Springer, 2014.

[5] N. Alexopoulos, S. M. Habib, S. Schulz, and M. Mühlhäuser. M-STAR: A modular, evidence-based software trustworthiness framework. *CoRR*, abs/1801.05764, 2018.

[6] M. Amith, K. Fujimoto, R. Mauldin, and C. Tao. Friend of a friend with benefits ontology (FOAF+): extending a social network ontology for public health. *BMC Medical Informatics Decis. Mak.*, 20-S(10):269, 2020.

[7] F. J. Aragó-Monzonís, L. Domínguez-García, A. Basurte-Durán, R. Ocaña, and V. Giralt. *SEAL Project: User-centric Application of Linked Digital Identity for Students and Citizens*, 2020. `https://project-seal.eu/node/143`.

[8] M. Arenas, B. C. Grau, E. Kharlamov, S. Marciuska, and D. Zheleznyakov. Faceted search over RDF-based knowledge graphs. *J. Web Semant.*, 37-38:55–74, 2016.

[9] Aristotle. *Prior Analytics*. Hackett Publishing Company, PO Box 44937 Indianapolis, Indiana, 46204 USA, 1989.

[10] R. C. Arkin, P. Ulam, and A. R. Wagner. Moral decision making in autonomous systems: Enforcement, moral emotions, dignity, trust, and deception. *Proceedings of the IEEE*, 100(3):571–589, 2012.

[11] D. Artz and Y. Gil. A survey of trust in computer science and the semantic web. *J. Web Sem.*, 5(2):58–71, 2007.

[12] Y. Ashibani and Q. H. Mahmoud. Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68:81–97, 2017.

[13] A. Avizienis, J. Laprie, B. Randell, and C. E. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Sec. Comput.*, 1(1):11–33, 2004.

[14] R. Axelrod. The future of cooperation. In *Proceedings of the IEEE Congress on Evolutionary Computation, CEC 2004, 19-23 June 2004, Portland, OR, USA*. IEEE, 2004.

[15] R. Axelrod and W. Hamilton. The evolution of cooperation. *Science*, 211(4489):1390–1396, 1981.

[16] F. Baader, D. Calvanese, D. L. McGuinness, D. Nardi, and P. F. Patel-Schneider, editors. *The Description Logic Handbook: Theory, Implementation, and Applications*. Cambridge University Press, New York, NY, USA, 2003.

[17] M. Bacharach. How human trusters assess trustworthiness in quasi-virtual contexts. In R. Falcone, K. S. Barber, L. Korba, and M. P. Singh, editors, *Trust, Reputation, and Security: Theories and Practice, AAMAS 2002 International Workshop, Bologna, Italy, July 15, 2002, Selected and Invited Papers*, volume 2631 of *Lecture Notes in Computer Science*, pages 1–7. Springer, 2002.

[18] M. Bacharach and D. Gambetta. *Trust in Signs*, pages 148–184. Russell Sage Foundation, 2001.

[19] M. Balduccini, E. Griffor, M. Huth, C. Vishik, M. Burns, and D. A. Wollman. Ontology-based reasoning about the trustworthiness of cyber-physical systems. *CoRR*, abs/1803.07438, 2018.

[20] S. Balfe, E. Gallery, C. J. Mitchell, and K. G. Paterson. Challenges for trusted computing. *IEEE Secur. Priv.*, 6(6):60–66, 2008.

[21] B. Barber. *Logic and Limits of Trust*. New Jersey: Rutgers University Press, 1983.

[22] A. Barenghi, A. D. Federico, G. Pelosi, and S. Sanfilippo. Challenging the trustworthiness of PGP: is the web-of-trust tear-proof? In G. Pernul, P. Y. A. Ryan, and E. R. Weippl, editors, *Computer Security — ESORICS 2015 — 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I*, volume 9326 of *Lecture Notes in Computer Science*, pages 429–446. Springer, 2015.

[23] C. d. S. baron de Montesquieu. The Spirit of Laws. Cambridge Texts in the History of Political Thought, 1750.

[24] J. Barwise. *An Introduction to First-Order Logic*. North-Holland, 1982.

[25] D. A. Basin, S. J. Burri, and G. Karjoth. Dynamic enforcement of abstract separation of duty constraints. In M. Backes and P. Ning, editors, *Computer Security — ESORICS 2009, 14th European Symposium on Research in Computer Security, Saint-Malo, France, September 21-23, 2009. Proceedings*, volume 5789 of *Lecture Notes in Computer Science*, pages 250–267. Springer, 2009.

[26] J. B. Bernabé, G. M. Pérez, and A. F. Skarmeta-Gómez. Intercloud trust and security decision support system: an ontology-based approach. *J. Grid Comput.*, 13(3):425–456, 2015.

[27] J. Bernal Bernabe, G. Martinez Perez, and A. F. Skarmeta Gomez. Intercloud Trust and Security Decision Support System: an Ontology-based Approach. *JOURNAL OF GRID COMPUTING*, 13(3, SI):425–456, SEP 2015.

[28] Bernardo Cuenca Grau. OWL 2 Web Ontology Language Tractable Fragments (Second Edition). `https://www.w3.org/2007/OWL/wiki/Tractable_Fragments`, 2004. Accessed: 2020-06-04.

[29] T. Berners-Lee, R. Fielding, and L. Masinter. Uniform Resource Identifier (URI): Generic Syntax. RFC 3986, RFC Editor, January 2005. `http://www.rfc-editor.org/rfc/rfc3986.txt`.

[30] T. Berners-Lee, J. Hendler, O. Lassila, et al. The semantic web. *Scientific american*, 284(5):28–37, 2001.

[31] B. Bishop, A. Kiryakov, D. Ognyanov, I. Peikov, Z. Tashev, and R. Velkov. FactForge: A fast track to the Web of data. *Semantic Web*, 2(2):157–166, 2011.

[32] B. Bishop, A. Kiryakov, Z. Tashev, M. Damova, and K. I. Simov. OWLIM reasoning over FactForge. In I. Horrocks, M. Yatskevich, and E. Jiménez-Ruiz, editors, *Proceedings of*

the 1st International Workshop on OWL Reasoner Evaluation (ORE-2012), Manchester, UK, July 1st, 2012, volume 858 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2012.

[33] J. Blasco Alís, J. C. H. Castro, J. E. Tapiador, and A. Ribagorda. Bypassing information leakage protection with trusted applications. *Comput. Secur.*, 31(4):557–568, 2012.

[34] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In *1996 IEEE Symposium on Security and Privacy, May 6-8, 1996, Oakland, CA, USA*, pages 164–173. IEEE Computer Society, 1996.

[35] A. Boer, R. Winkels, and F. Vitali. Metalex xml and the legal knowledge interchange format. In P. Casanovas, G. Sartor, N. Casellas, and R. Rubino, editors, *Computable Models of the Law*, pages 21–41, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[36] A. Borgida. On the relative expressiveness of description logics and predicate logics. *Artif. Intell.*, 82(1-2):353–367, 1996.

[37] D. Brickley and L. Miller. FOAF Vocabulary Specification 0.99. 2014. `http://xmlns.com/foaf/spec/`.

[38] M. Burrows, M. Abadi, and R. M. Needham. Authentication: A practical study in belief and action. In *Proceedings of the 2nd Conference on Theoretical Aspects of Reasoning about Knowledge, Pacific Grove, CA, USA, March 1988*, pages 325–342, 1988.

[39] M. Burrows, M. Abadi, and R. M. Needham. A logic of authentication. *ACM Trans. Comput. Syst.*, 8(1):18–36, 1990.

[40] G. W. Bush. Homeland Security Presidential Directive-12, 2004. `https://www.dhs.gov/homeland-security-presidential-directive-12`.

[41] CABforum. Ev SSL Certificate Guidelines version 1.7.1. Available from: https://cabforum.org/ (accessed 10 February 2021).

[42] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer. OpenPGP Message Format. RFC 4880, RFC Editor, November 2007. `http://www.rfc-editor.org/rfc/rfc4880.txt`.

[43] Q. H. Cao, I. Khan, R. Farahbakhsh, G. Madhusudan, G. M. Lee, and N. Crespi. A trust model for data sharing in smart cities. In *2016 IEEE International Conference on Communications, ICC 2016, Kuala Lumpur, Malaysia, May 22-27, 2016*, pages 1–7, 2016.

[44] O. Carpanini and F. Cerutti. Towards an ontology of trust for situational understanding. In F. Chao, S. Schockaert, and Q. Zhang, editors, *Advances in Computational Intelligence Systems — Contributions Presented at the 17th UK Workshop on Computational Intelligence, September 6-8, 2017, Cardiff, UK*, volume 650 of *Advances in Intelligent Systems and Computing*, pages 290–296. Springer, 2017.

[45] J. J. Carroll, C. Bizer, P. J. Hayes, and P. Stickler. Named graphs, provenance and trust. In A. Ellis and T. Hagino, editors, *Proceedings of the 14th international conference on World Wide Web, WWW 2005, Chiba, Japan, May 10-14, 2005*, pages 613–622. ACM, 2005.

[46] C. Castelfranchi and R. Falcone. Trust and control: A dialectic link. *Applied Artificial Intelligence*, 14(8):799–823, 2000.

[47] A. Censi, K. Slutsky, T. Wongpiromsarn, D. S. Yershov, S. Pendleton, J. G. M. Fu, and E. Frazzoli. Liability, ethics, and culture-aware behavior specification using rulebooks. *CoRR*, abs/1902.09355, 2019.

[48] D. Ceolin, P. T. Groth, and W. R. van Hage. Calculating the trust of event descriptions using provenance. In S. S. Sahoo, J. Zhao, P. Missier, and J. M. Gómez-Pérez, editors, *Proceedings of the Second International Workshop on the role of Semantic Web in Provenance Management, SWPM@ISWC 2010, Shanghai, China, November 7, 2010*, volume 670 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2010.

[49] D. Ceolin, A. Nottamkandath, and W. Fokkink. Bridging gaps between subjective logic and semantic web. In F. Bobillo, R. N. Carvalho, P. C. G. da Costa, C. d'Amato, N. Fanizzi, K. B. Laskey, K. J. Laskey, T. Lukasiewicz, M. Nickles, and M. Pool, editors, *Uncertainty Reasoning for the Semantic Web III — ISWC International Workshops, URSW 2011-2013, Revised Selected Papers*, volume 8816 of *Lecture Notes in Computer Science*, pages 242–264. Springer, 2014.

[50] D. Ceolin, A. Nottamkandath, and W. Fokkink. Efficient semi-automated assessment of annotations trustworthiness. *Journal of Trust Management, https://journaloftrustmanagement.springeropen.com*, 2014.

[51] D. Ceolin, A. Nottamkandath, W. Fokkink, and V. Maccatrozzo. Towards the definition of an ontology for trust in (web) data. In *Proceedings of the 10th International Workshop on Uncertainty Reasoning for the Semantic Web (URSW 2014) co-located with the 13th International Semantic Web Conference (ISWC 2014), Riva del Garda, Italy, October 19, 2014.*, pages 73–78, 2014.

[52] V.-I. C.G. *Bonds of mutual trust: the cultural systems of rotating credit associations among urban Mexicans and Chicanos*. New Brunswick, N.J., Rutgers University Press, 1983.

[53] A. Chakravarthy, S. Wiegand, X. Chen, B. Nasser, and M. Surridge. Trustworthy systems design using semantic risk modelling. In C. University, editor, *Working Papers of the Sustainable Society Network+ Vol. 3 February 2015*, pages 49–81. Coventry University, 2015.

[54] C. Chen, C. Mitchell, and S. Tang. *Building general purpose security services on trusted computing*, volume 7222 of *Lecture Notes in Computer Science*, pages 16–31. Springer-Verlag, 2012.

[55] I. Chen, F. Bao, and J. Guo. Trust-based service management for social internet of things systems. *IEEE Transactions on Dependable and Secure Computing*, 13(06):684–696, nov 2016.

[56] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56:1–27, 2016.

[57] J. Cho, K. S. Chan, and S. Adali. A survey on trust modeling. *ACM Comput. Surv.*, 48(2):28:1–28:40, 2015.

[58] J. Cho and I. Chen. Provest: Provenance-based trust model for delay tolerant networks. *IEEE Transactions on Dependable and Secure Computing*, 15(01):151–165, jan 2018.

[59] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC 3647, RFC Editor, November 2003. `http://www.rfc-editor.org/rfc/rfc3647.txt`.

[60] D. D. Clark and D. R. Wilson. A comparison of commercial and military computer security policies. In *Proceedings of the 1987 IEEE Symposium on Security and Privacy, Oakland, California, USA, April 27-29, 1987*, pages 184–195, 1987.

[61] T. Coffey, P. Saidha, and P. Burrows. Analysing the security of a non-repudiation communication protocol with mandatory proof of receipt. In *Proceedings of the 1st Intenational Symposium on Information and Communication Technologies, Dublin, Ireland, September 24-26, 2003*, pages 351–356, 2003.

[62] P. Cofta. *Trust, Complexity and Control: Confidence in a Convergent World*. Wiley, 2007.

[63] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Dinternet x.509 public key infrastructure certificate and certificate revocation list (CRL) profile. RFC 5280, RFC Editor, May 2008. http://www.rfc-editor.org/rfc/rfc5280.txt.

[64] H. M. Cooper. Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge, Technology & Policy*, 1(1):104–126, 1988.

[65] M. Damova, K. I. Simov, Z. Tashev, and A. Kiryakov. FactForge: Data Service or the Diversity of Inferred Knowledge over LOD. In *Artificial Intelligence: Methodology, Systems, and Applications - 15th International Conference, AIMSA 2012, Varna, Bulgaria, September 12-15, 2012. Proceedings*, pages 145–151, 2012.

[66] DCMI Usage Board. DCMI Metadata Terms. https://dublincore.org/specifications/dublin-core/dcmi-terms/, 2020. Accessed: 2020-12-01.

[67] O. Delos, T. Debusschere, M. D. Soete, J. Dumortier, R. Genghini, H. Graux, S. Lacroix, G. Ramunno, M. Sel, and P. V. Eecke. A pan-european framework on electronic identification and trust services for electronic transactions in the internal market. In S. Paulus, N. Pohlman, and H. Reimer, editors, *Securing business processes*, pages 173–195. Vieweg+Tuebner, Springer Science+Business Media, 2015.

[68] A. Dent and C. Mitchell. *User's guide to cryptography and standards*. Artech House, 2005.

[69] M. Deutsch. *Cooperation and trust: Some theoretical notes.* Univer. Nebraska Press, 1962.

[70] M. Deutsch. *The resolution of conflict: Constructive and destructive processes*. Yale University Press, 1977.

[71] C. E. Dickerson, S. Ji, and R. Roslan. Formal Methods for a System of Systems Analysis Framework Applied to Traffic Management. In *2016 11TH Systems of system engineering conference (SOSE), IEEE*. IEEE, 2016.

[72] L. Ding, P. Kolari, T. Finin, A. Joshi, Y. Peng, and Y. Yesha. On homeland security and the semantic web: A provenance and trust aware inference framework. In *AI Technologies for Homeland Security, Papers from the 2005 AAAI Spring Symposium, Technical Report SS-05-01, Stanford, California, USA, March 21-23, 2005*, pages 157–160. AAAI, 2005.

[73] L. Ding, L. Zhou, T. W. Finin, and A. Joshi. How the semantic web is being used: An analysis of FOAF documents. In *38th Hawaii International Conference on System*

Sciences (HICSS-38 2005), CD-ROM / Abstracts Proceedings, 3-6 January 2005, Big Island, HI, USA, pages 113c – 113c. IEEE Computer Society, 2005.

[74] J. J. Douceur. The Sybil Attack. In *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, January 2002.

[75] J. R. Douceur. The Sybil Attack. In P. Druschel, M. F. Kaashoek, and A. I. T. Rowstron, editors, *Peer-to-Peer Systems, First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 7-8, 2002, Revised Papers*, volume 2429 of *Lecture Notes in Computer Science*, pages 251–260. Springer, 2002.

[76] EA. *EA Resolution 2014 (34) 22*. European cooperation for Accreditation, 2014. https://european-accreditation.org/wp-content/uploads/2018/10/34th-ea-ga-approved-resolutions-.pdf.

[77] EDM Council. Financial Industry Business Ontology: Foundations Version 1.2. https://www.omg.org/spec/EDMC-FIBO/FND/1.2/PDF, 2017. Accessed: 2020-12-02.

[78] EDM Council. Financial Industry Business Ontology: Business Entities Version 1.1. https://www.omg.org/spec/EDMC-FIBO/BE/1.1/PDF, 2018. Accessed: 2020-12-02.

[79] EDM Council. Financial Industry Business Ontology: Indices and Indicators Version 1.0. https://www.omg.org/spec/EDMC-FIBO/IND/1.0/PDF, 2018. Accessed: 2020-12-02.

[80] eIDAS eID Technical Subgroup. eIDAS Cryptographic Requirement v1.2. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile, 2019. Accessed: 2020-11-28.

[81] eIDAS eID Technical Subgroup. eIDAS Interoperability Architecture v1.2. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile, 2019. Accessed: 2020-11-28.

[82] eIDAS eID Technical Subgroup. eIDAS Message Format v1.2. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile, 2019. Accessed: 2020-11-28.

[83] eIDAS eID Technical Subgroup. eIDAS SAML Attribute Profile v1.2. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile, 2019. Accessed: 2020-11-28.

[84] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[85] F. B. en Ondersteuning. Federal Authorization Service OIDC onboarding. Technical report, FPS BOSA, 2019.

[86] N. Engelbertz, N. Erinola, D. Herring, J. Somorovsky, V. Mladenov, and J. Schwenk. Security Analysis of eIDAS – The Cross-Country Authentication Scheme in Europe. In *12th USENIX Workshop on Offensive Technologies (WOOT 18)*, Baltimore, MD, Aug. 2018. USENIX Association.

[87] ETSI. *Electronic Signatures and Infrastructures (ESI) Trust Service Provider Conformity Assessment — Requirements for conformity assessment bodies assessing Trust Service Providers*, 2015. EN 319 403.

[88] ETSI. *Electronic Signatures and Infrastructures (ESI) Trust Service Provider Conformity Assessment — Requirements for conformity assessment bodies assessing Trust Service Providers*, 2015. TS 319 403.

[89] ETSI. *Electronic Signatures and Infrastructures (ESI) Trusted Lists V2.1.1*, 2015. TS 119 612.

[90] ETSI. *Electronic Signatures and Infrastructures (ESI) General Policy Requirements for Trust Service Providers*, 2016. TS 319 401.

[91] ETSI. *Electronic Signatures and Infrastructures (ESI) General Policy Requirements for Trust Service Providers*, 2016. EN 319 401.

[92] ETSI. *Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Trust Service Providers issuing certificates — Part 1 General requirements*, 2016. TS 319 411-1.

[93] ETSI. *Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Trust Service Providers issuing certificates — Part 1 General requirements*, 2016. EN 319 411-1.

[94] ETSI. *Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Trust Service Providers issuing certificates — Part 2 Requirements for trust service providers issuing EU qualified certificates*, 2016. TS 319 411-2.

[95] ETSI. *Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Trust Service Providers issuing certificates — Part 2 Requirements for trust service providers issuing EU qualified certificates*, 2016. EN 319 411-2.

[96] ETSI. *Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Trust Service Providers issuing time stamps*, 2016. TS 319 421.

[97] ETSI. *Electronic Signatures and Infrastructures (ESI) — Trust Service Providers Conformity Assessment Part 2 Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates*, 2018. TS 119 403-2.

[98] ETSI. *Electronic Signatures and Infrastructures (ESI) Trust Service Provider Conformity Assessment — Requirements for conformity assessment bodies assessing Trust Service Providers*, 2020. TS 319 403-1.

[99] ETSI. *ETSI TR 103 684 V1.1.1 Global Acceptance of EU Trust Services*. ETSI, 2020. TR 103 684 V1.1.1.

[100] European Parliament and European Council. *Regulation EC 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance related to the marketing of products and repealing Regulation EEC 339/93 (text with EEA relevance)*. EU, 2008. Official Journal of the European Union, OJ L 218, 13.8.2008, p. 30-47.

[101] European Parliament and European Council. *EU 2016/679 Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. European Commission DG Justice, 2016. Official Journal of the European Union, L 119, 4 May 2016.

[102] European Parliament and European Council. *Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information*. EU, 2019. Official Journal of the European Union, OJ L 172, 26.6.2019, p. 56-83.

[103] European Union. *EU 910/2014 Regulation of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. DG CONNECT, 2014. OJ L 257, 28.8.2014, p. 73 114.

[104] European Union. *EU 2015/1501, Implementing Act on interoperability framework*. European Commission, 2015. EU 2015/1501.

[105] European Union. *EU 2015/1502, Implementing Act on identity Levels of Assurance*. European Commission, 2015. EU 2015/1502.

[106] European Union. *EU 2015/1505, Implementing Act on Trusted List formats*. European Commission, 2015. EU 2015/1505.

[107] European Union. *EU 2015/1506, Implementing Act on formats for signatures and seals*. European Commission, 2015. EU 2015/1506.

[108] European Union. *EU 2015/1984, Implementing Act defining the circumstances, formats and procedures of notification*. European Commission, 2015. EU 2015/1984.

[109] European Union. *EU 2015/296, Implementing Decision on Member State cooperation for identity*. European Commission, 2015. EU 2015/296.

[110] European Union. *EU 2015/806, Implementing act on trust mark*. European Commission, 2015. EU 2015/806.

[111] European Union. *EU 2016/650, Standards for the security assessment of qualified signature and seal creation devices*. European Commission, 2016. EU 2016/650.

[112] W. Fan and H. G. Perros. A novel trust management framework for multi-cloud environments based on trust service providers. *Knowl.-Based Syst.*, 70:392–406, 2014.

[113] H. Fang, J. Zhang, and M. Sensoy. A generalized stereotype learning approach and its instantiation in trust modeling. *Electronic Commerce Research and Applications*, 30:149–158, JUL-AUG 2018.

[114] H. Fatemi, M. van Sinderen, and R. J. Wieringa. A trust ontology for business collaborations. In K. Sandkuhl, U. Seigerroth, and J. Stirna, editors, *Short Paper Proceedings of the 5th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling, Rostock, Germany, November 7-8, 2012*, volume 933 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2012.

[115] FEDICT. Federal Portal Civil Servant and Citizen Authentication Service Cookbook. Technical report, FEDICT, 2007.

[116] M. S. Ferdous, G. Norman, A. Jøsang, and R. Poet. Mathematical modelling of trust issues in federated identity management. In C. D. Jensen, S. Marsh, T. Dimitrakos, and Y. Murayama, editors, *Trust Management IX — 9th IFIP WG 11.11 International Conference, IFIPTM 2015, Hamburg, Germany, May 26-28, 2015, Proceedings*, volume 454 of *IFIP Advances in Information and Communication Technology*, pages 13–29. Springer, 2015.

[117] P. Fogliaroni, F. D'Antonio, and E. Clementini. Data trustworthiness and user reputation as indicators of VGI quality. *Geo-Spatial Information Science*, 21(3, SI):213–233, 2018.

[118] A. Fuchs, S. Gürgens, and C. Rudolph. A formal notion of trust–enabling reasoning about security properties. In *Trust Management IV*, pages 200–215. Springer, 2010.

[119] D. Gambetta. Can we trust trust? In D. Gambetta, editor, *Trust: Making and Breaking Cooperative Relations*, pages 213–237. Basil Blackwell, Oxford, 1988.

[120] H. Gang, B. Yinfeng, Z. Kuanjiu, W. Jie, L. Mingchu, and L. Zihao. Energy Consumption Analysis Method of CPS Software Based on Architecture Modeling. In Jia, XH and Dillion, T and Li, KC and Zhang, Y and Kato, N and Wu, K and Zhang, YQ, editor, *2015 Ninth International Conference on Frontier of Computer Science and Technology FCST 2015*, pages 34–39. Liaoning Normal Univ, 2015. 9th International Conference on Frontier of Computer Science and Technology, Dalian, Peoples Republic of China, August 26-28, 2015.

[121] Y. Gil and D. Artz. Towards content trust of web resources. *J. Web Semant.*, 5(4):227–239, 2007.

[122] GLEIF. Entity Legal Form Ontology — Who Is Who. `https://www.gleif.org/ontology/EntityLegalForm-v1.0/EntityLegalForm/`. Accessed: 2020-12-02.

[123] GLEIF. Global Legal Entity Identifier Foundation Level 1 Ontology — Who Is Who. `https://www.gleif.org/ontology/v1.0/L1/`. Accessed: 2020-12-02.

[124] GLEIF. Global Legal Entity Identifier Foundation Level 2 Ontology — Who Owns Whom. `https://www.gleif.org/ontology/v1.0/L2/`. Accessed: 2020-12-02.

[125] GLEIF. Global Legal Entity Identifier Foundation Registration Authority Ontology. `https://www.gleif.org/ontology/v1.0/RegistrationAuthority/index-en.html`. Accessed: 2020-12-02.

[126] V. D. Gligor, S. I. Gavrila, and D. F. Ferraiolo. On the formal definition of separation-of-duty policies and their composition. In *Security and Privacy — 1998 IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 3-6, 1998, Proceedings*, pages 172–183. IEEE Computer Society, 1998.

[127] B. Glimm, I. Horrocks, B. Motik, G. Stoilos, and Z. Wang. Hermit: An OWL 2 reasoner. *J. Autom. Reasoning*, 53(3):245–269, 2014.

[128] J. Golbeck, B. Parsia, and J. A. Hendler. Trust networks on the semantic web. In M. Klusch, S. Ossowski, A. Omicini, and H. Laamanen, editors, *Cooperative Information Agents VII, 7th International Workshop, CIA 2003, Helsinki, Finland, August 27-29, 2003, Proceedings*, volume 2782 of *Lecture Notes in Computer Science*, pages 238–249. Springer, 2003.

[129] A. Goldsteen, M. Moffie, T. Bandyszak, N. G. Mohammadi, X. Chen, S. Meichanetzoglou, S. Ioannidis, and P. Chatziadam. A tool for monitoring and maintaining system thrustworthiness at runtime. In *Joint Proceedings of REFSQ-2015 Workshops, Research Method Track, and Poster Track co-located with the 21st International Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2015), Essen, Germany, March 23, 2015.*, pages 142–147, 2015.

[130] D. Gollmann. *Computer Security*. John Wiley and Sons, 1999.

[131] D. Gollmann. Why trust is bad for security. *Electronic Notes in Theoretical Computer Science*, 157(3):3 — 9, 2006. Proceedings of the First International Workshop on Security and Trust Management (STM 2005).

[132] L. Gong, M. Mueller, H. Prafullchandra, and R. Schemers. Going beyond the sandbox: An overview of the new security architecture in the java development kit 1.2. In *1st USENIX Symposium on Internet Technologies and Systems, USITS'97, Monterey, California, USA, December 8-11, 1997*. USENIX, 1997.

[133] L. Gong, R. M. Needham, and R. Yahalom. Reasoning about belief in cryptographic protocols. In *Proceedings of the 1990 IEEE Symposium on Security and Privacy, Oakland, California, USA, May 7-9, 1990*, pages 234–248, 1990.

[134] P. Govindaraj. A review on various trust models in cloud environment. *Journal of Engineering Science and Technology Review*, 10(2):213–219, 2017.

[135] P. A. Grassi, M. E. Garcia, and J. L. Fenton. *Digital Identity Guidelines. NIST Special Publication SP-800-63-3*. National Institute of Standards and Technology, 2017.

[136] E. Griffor, C. Greer, D. Wollman, and M. Burns. *Framework for Cyber-Physical Systems: Volume 1, Overview. Technical Report NIST-SP-1500-201*. National Institute of Standards and Technology, 2017.

[137] B. N. Grosof, I. Horrocks, R. Volz, and S. Decker. Description Logic Programs: combining logic programs with description logic. In *Proceedings of the Twelfth International World Wide Web Conference, WWW 2003, Budapest, Hungary, May 20-24, 2003*, pages 48–57, 2003.

[138] S. M. Habib, N. Alexopoulos, M. M. Islam, J. Heider, S. Marsh, and M. Mühlhäuser. Trust4app: Automating trustworthiness assessment of mobile applications. In *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineer-*

ing, TrustCom/BigDataSE 2018, New York, NY, USA, August 1-3, 2018, pages 124–135. IEEE, 2018.

[139] S. M. Habib, S. Hauke, S. Ries, and M. Mühlhäuser. Trust as a facilitator in cloud computing: a survey. *J. Cloud Computing*, 1:19, 2012.

[140] S. M. Habib, F. Volk, S. Hauke, and M. Mühlhäuser. Computational trust methods for security quantification in the cloud ecosystem. In R. K. L. Ko and K. R. Choo, editors, *The Cloud Security Ecosystem — Technical, Legal, Business and Management Issues.*, pages 463–493. Elsevier, 2015.

[141] H. Halpin. Vision: A critique of immunity passports and W3C decentralized identifiers. In T. van der Merwe, C. J. Mitchell, and M. Mehrnezhad, editors, *Security Standardisation Research — 6th International Conference, SSR 2020, London, UK, November 30 — December 1, 2020, Proceedings*, volume 12529 of *Lecture Notes in Computer Science*, pages 148–168. Springer, 2020.

[142] C. Hanson, T. Berners-Lee, L. Kagal, G. J. Sussman, and D. J. Weitzner. Data-purpose algebra: Modeling data usage policies. In *8th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2007), 13-15 June 2007, Bologna, Italy*, pages 173–177, 2007.

[143] O. Hartig. Querying Trust in RDF data with tSPARQL. In L. Aroyo, P. Traverso, F. Ciravegna, P. Cimiano, T. Heath, E. Hyvönen, R. Mizoguchi, E. Oren, M. Sabou, and E. Simperl, editors, *The Semantic Web: Research and Applications*, volume 5554 of *Lecture Notes in Computer Science*, pages 5–20. Springer Berlin Heidelberg, 2009.

[144] HCCH. *Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents*. Hague Conference on Private International Law, 1961. Last retrieved on 30/12/2020 from https://www.hcch.net/en/instruments/conventions/full-text/.

[145] T. Heath and E. Motta. The hoonoh ontology for describing trust relationships in information seeking. *Personal Identification and Collaborations: Knowledge Mediation and Extraction (PICKME2008)*, 2008.

[146] M. Henderson, R. S. Coulter, E. Dawson, and E. Okamoto. Modelling trust structures for public key infrastructures. In *Information Security and Privacy, 7th Australian Conference, ACISP 2002, Melbourne, Australia, July 3-5, 2002, Proceedings*, pages 56–70, 2002.

[147] J. Heurix, P. Zimmermann, T. Neubauer, and S. Fenz. A taxonomy for privacy enhancing technologies. *Computers & Security*, 53:1–17, 2015.

[148] P. Hitzler, M. Krötzsch, and S. Rudolph. *Foundations of Semantic Web Technologies*. Chapman & Hall/CRC, 2009.

[149] A. Hodges. Alan Turing. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2019 edition, 2019.

[150] P. Hoffman, L. Masinter, and J. Zawinski. The mailto URL scheme. RFC 2368, RFC Editor, November 1998. `http://www.rfc-editor.org/rfc/rfc2368.txt`.

[151] G. Hogben and M. Dekker. *Procure Secure: a guide to monitoring of security service levels in cloud contracts*, 2012. Available from: `https://www.enisa.europa.eu/publications/` (last accessed 12 March 2021).

[152] M. Horridge and M. A. Musen. Snap-SPARQL: A Java framework for working with SPARQL and OWL. In *Ontology Engineering — 12th International Experiences and Directions Workshop on OWL, OWLED 2015, co-located with ISWC 2015, Bethlehem, PA, USA, October 9-10, 2015, Revised Selected Papers*, pages 154–165, 2015.

[153] I. Horrocks, O. Kutz, and U. Sattler. The even more irresistible SROIQ. In *Proceedings, Tenth International Conference on Principles of Knowledge Representation and Reasoning, Lake District of the United Kingdom, June 2-5, 2006*, pages 57–67, 2006.

[154] I. Horrocks and P. F. Patel-Schneider. A proposal for an OWL rules language. In S. I. Feldman, M. Uretsky, M. Najork, and C. E. Wills, editors, *Proceedings of the 13th international conference on World Wide Web, WWW 2004, New York, NY, USA, May 17-20, 2004*, pages 723–731. ACM, 2004.

[155] J. Huang and M. S. Fox. An ontology of trust: formal semantics and transitivity. In M. S. Fox and B. Spencer, editors, *Proceedings of the 8th International Conference on Electronic Commerce: The new e-commerce — Innovations for Conquering Current Barriers, Obstacles and Limitations to Conducting Successful Business on the Internet, 2006, Fredericton, New Brunswick, Canada, August 13-16, 2006*, volume 156 of *ACM International Conference Proceeding Series*, pages 259–270. ACM, 2006.

[156] J. Huang and D. M. Nicol. An anatomy of trust in public key infrastructure. *International Journal of Critical Infrastructures*, 13:238, 01 2017.

[157] J. Huang and D. Nicol. A Calculus of Trust and its Application to PKI and identity management. In ACM, editor, *IDTrust 2009*. ACM, 2009.

[158] J. Huang, M. D. Seck, and A. V. Gheorghe. Towards trustworthy smart cyber-physical-social systems in the era of internet of things. In *11th System of Systems Engineering Conference, SoSE 2016, Kongsberg, Norway, June 12-16, 2016*, pages 1–6, 2016.

[159] J. Huerta, S. Schade, and C. Granell, editors. *Connecting a Digital Europe Through Location and Place — International AGILE'2014 Conference, Castellon, Spain, 13-16 June, 2014*, Lecture Notes in Geoinformation and Cartography. Springer, 2014.

[160] J. H. Huh and A. Martin. Towards a Trustable Virtual Organisation. pages 425–431, Los Alamitos, CA, USA, November 2009. IEEE Computer Society.

[161] D. Hühnlein, T. Frosch, J. Schwenk, C. Piswanger, M. Sel, T. Hühnlein, T. Wich, D. Nemmert, R. Lottes, J. Somorovsky, V. Mladenov, C. Condovici, H. Leitold, S. Stalla-Bourdillon, N. Tsakalakis, J. Eichholz, F. Kamm, A. Kühne, D. Wabisch, R. Dean, J. Shamah, M. Kapanadze, N. Ponte, J. Martins, R. Portela, C. Karabat, S. Stojicic, S. Nedeljkovic, V. Bouckaert, A. Defays, B. Anderson, M. Jonas, C. Hermanns, T. Schubert, D. Wegener, and A. Sazonov. FutureTrust — Future Trust Services for Trustworthy Global Transactions. In D. Hühnlein, H. Roßnagel, C. H. Schunck, and M. Talamo, editors, *Open Identity Summit 2016, 13.-14. October 2016, Rome, Italy*, volume P-264 of *LNI*, pages 27–41. GI, 2016.

[162] ILNAS. *ILNAS/PSCQ/Pr001 Supervision of Qualified Trust Service Providers (QTSPs)*. Luxembourg Institute of Standardisation, Accreditation, Safety and Quality of Products and Services, 2019. Accessed= 2021-02-12.

[163] Information Technology Laboratory. *Secure Hash Standard (SHS)*. National Institute of Standards and Technology, 2015. `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf`.

[164] R. Ismail and A. Jøsang. The beta reputation system. In *15th Bled eConference: eReality: Constructing the eEconomy, Bled, Slovenia, June 17-19, 2002*, page 41, 2002.

[165] ISO. *ISO 17422: Financial Services — Legal entity identifier (LEI)*.

[166] ISO. *ISO 20275:2017: Financial Services — Entity legal forms*.

[167] ISO. *ISO 21188:2018 Public key infrastructure for financial services — Practices and policy framework*.

[168] ISO. *ISO/IEC 101118-3:2018 IT Security Techniques — Hash Functions — Part 3 Dedicated Hash Functions*.

[169] ISO. *ISO/IEC 11889-1:2009 Information Technology — TPM Library Part 1: Overview*.

[170] ISO. *ISO/IEC 11889-2:2009 Information Technology — TPM Library Part 2: Design Principles*.

[171] ISO. *ISO/IEC 11889-3:2009 Information Technology — TPM Library Part 3: Structures*.

[172] ISO. *ISO/IEC 11889-4:2009 Information Technology — TPM Library Part 4: Commands*.

[173] ISO. *ISO/IEC 17000: Conformity Assessment — Vocabulary and general principles*.

[174] ISO. *ISO/IEC 17011:2017(E) Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies*.

[175] ISO. *ISO/IEC 17021-1:2015(E) Conformity assessment — Requirements for bodies providing audit and certification of management systems - Part 1 Requirements*.

[176] ISO. *ISO/IEC 17065:2012(E) Conformity assessment — Requirements for bodies certifying products, processes and services*.

[177] ISO. *ISO/IEC 27001:2013(E) Information technology — Security techniques — Information security management systems — Requirements*.

[178] ISO. *ISO/IEC 27006:2015(E) Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*.

[179] ISO. *ISO/IEC 27014:2013(E) Information technology — Security techniques — Governance of information security*.

[180] ISO. *ISO/IEC 29003:2018(E) Information technology — Security techniques — Identity proofing*.

[181] ISO. *ISO/IEC 29115:2013(E) Information technology — Security techniques — Entity authentication — assurance framework*.

[182] ISO. *ISO/IEC 8859-1:1998 Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*.

[183] ISO. *ISO/IEC PRF 21838-1: Information Technology — Top-level ontologies (TLO) — Part 1 Requirements*, 2020.

[184] ISO. *ISO/IEC PRF 21838-2: Information Technology — Top-level ontologies (TLO) — Part 2 Basic Formal Ontology (BFO)*, 2020.

[185] I. Jacobi, L. Kagal, and A. Khandelwal. Rule-based trust assessment on the semantic web. In *Rule-Based Reasoning, Programming, and Applications — 5th International Symposium, RuleML 2011 — Europe, Barcelona, Spain, July 19-21, 2011. Proceedings*, pages 227–241, 2011.

[186] S. Javanmardi, M. Shojafar, S. Shariatmadari, and S. S. Ahrabi. FRTRUST: a fuzzy reputation based model for trust management in semantic P2P grids. *CoRR*, abs/1404.2632, 2014.

[187] S. Jha, S. Sural, V. Atluri, and J. Vaidya. Specification and verification of separation of duty constraints in attribute-based access control. *IEEE Trans. Inf. Forensics Secur.*, 13(4):897–911, 2018.

[188] A. Jøsang. *Subjective Logic — A Formalism for Reasoning Under Uncertainty*. Artificial Intelligence: Foundations, Theory, and Algorithms. Springer, 2016.

[189] A. Jøsang and V. A. Bondi. Legal reasoning with subjective logic. *Artif. Intell. Law*, 8(4):289–315, 2000.

[190] A. Jøsang, R. Hayward, and S. Pope. Trust network analysis with subjective logic. In *Proceedings of the 29th Australasian Computer Science Conference — Volume 48*, ACSC '06, pages 85–94, Darlinghurst, Australia, Australia, 2006. Australian Computer Society, Inc.

[191] A. Jøsang and S. Lo Presti. Analysing the relationship between risk and trust. In *Trust Management, Second International Conference, iTrust 2004, Oxford, UK, March 29 — April 1, 2004, Proceedings*, pages 135–145, 2004.

[192] A. Jøsang, S. Marsh, and S. Pope. Exploring different types of trust propagation. In K. Stølen, W. H. Winsborough, F. Martinelli, and F. Massacci, editors, *Trust Management, 4th International Conference, iTrust 2006, Pisa, Italy, May 16-19, 2006, Proceedings*, volume 3986 of *Lecture Notes in Computer Science*, pages 179–192. Springer, 2006.

[193] L. Kagal, T. W. Finin, and A. Joshi. A policy language for a pervasive computing environment. In *4th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), 4-6 June 2003, Lake Como, Italy*, page 63, 2003.

[194] E. Kalemi and E. Martiri. FOAF-Academic Ontology: A vocabulary for the academic community. In F. Xhafa, L. Barolli, and M. Köppen, editors, *2011 Third International Conference on Intelligent Networking and Collaborative Systems (INCoS), Fukuoka, Japan, November 30 - Dec. 2, 2011*, pages 440–445. IEEE Computer Society, 2011.

[195] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in P2P networks. In *Proceedings of the Twelfth International World Wide Web Conference, WWW 2003, Budapest, Hungary, May 20-24, 2003*, pages 640–651, 2003.

[196] G. Karame and E. Androulaki. *Bitcoin and Blockchain Security*. Artech House, 2016.

[197] N. Karthik and V. S. Ananthanarayana. An Ontology Based Trust Framework for Sensor-Driven Pervasive Environment. In AlDabass, D and Shapiai, MI and Ibrahim, Z, editor, *2017 Asia Modelling Symposium (AMS 2017)*, pages 147–152, 2017.

[198] P. Karuna, H. Purohit, and V. Motti. UTPO: user's trust profile ontology — modeling trust towards online health information sources. *CoRR*, abs/1901.01276, 2019.

[199] Kieron O'Hara. A general definition of trust. `https://eprints.soton.ac.uk/341800/`, 2012. Accessed: 2021-04-21.

[200] Y. Kim, J.-S. Choi, and Y. Shin. Trustworthy Service Discovery for Dynamic Web Service Composition. *KSII Transactions on Internet and Information Systems*, 9(3):1260–1281, MAR 31 2015.

[201] S. Kirrane, A. Mileo, and S. Decker. Access control and the resource description framework: A survey. *Semantic Web*, 8(2):311–352, 2017.

[202] S. Kirrane, S. Villata, and M. d'Aquin. Privacy, security and policies: A review of problems and solutions with semantic web technologies. *Semantic Web*, 9(2):153–161, 2018.

[203] S. Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64:122–134, 2017.

[204] K. Kravari and N. Bassiliades. DISARM: A social distributed agent reputation model based on defeasible logic. *Journal of Systems and Software*, 117:130–152, JUL 2016.

[205] K. Kravari and N. Bassiliades. ORDAIN: an ontology for trust management in the internet of things — (short paper). In H. Panetto, C. Debruyne, W. Gaaloul, M. P. Papazoglou, A. Paschke, C. A. Ardagna, and R. Meersman, editors, *On the Move to Meaningful Internet Systems. OTM 2017 Conferences — Confederated International Conferences: CoopIS, C&TC, and ODBASE 2017, Rhodes, Greece, October 23-27, 2017, Proceedings, Part II*, volume 10574 of *Lecture Notes in Computer Science*, pages 216–223. Springer, 2017.

[206] G. Kreisel and J. L. Krivine. *Elements of Mathematical Logic: Model Theory*. Amsterdam: North Holland Pub. Co., 1967.

[207] S. Kripke. Naming and necessity. In D. Davidson and G. Harman, editors, *Semantics of natural language*, Synthese Library, pages 253–355. Reidel, Dordrecht, 1972.

[208] M. Krötzsch, F. Simancik, and I. Horrocks. A Description Logic Primer. *CoRR*, abs/1201.4089, 2012.

[209] J. Krutil, M. Kudelka, and V. Snásel. Web page classification based on schema.org collection. In *Fourth International Conference on Computational Aspects of Social Networks, CASoN 2012, Sao Carlos, Brazil, November 21-23, 2012*, pages 356–360. IEEE, 2012.

[210] R. Kuhn, V. Hu, T. Polk, and S.-J. Shang. *Managing Information Security Risk. NIST Special Publication SP-800-32*. National Institute of Standards and Technology, 2001.

[211] R. Küsters, T. Truderung, and A. Vogt. Accountability: definition and relationship to verifiability. In *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010*, pages 526–535, 2010.

[212] L. Lamport. The Part-Time Parliament. *ACM Trans. Comput. Syst.*, 16(2):133–169, 1998.

[213] L. Lamport, R. Shostak, and M. Pease. The Byzantine Generals problem. *ACM Transactions on Programming Languages and Systems*, 4/3:382–401, July 1982.

[214] J.-C. Laprie. *Dependability Its Attributes, Impairments and Means*. Springer, Berlin, Heidelberg, 1995.

[215] J. Li, Y. Bai, N. Zaman, and V. C. M. Leung. A decentralized trustworthy context and qos-aware service discovery framework for the internet of things. *IEEE Access*, 5:19154–19166, 2017.

[216] J. Li, C. Liu, and Z. Li. An ontology-based framework model for trustworthy software evolution. In L. Cao, J. Zhong, and Y. Feng, editors, *Advanced Data Mining and Applications — 6th International Conference, ADMA 2010, Chongqing, China, November 19-21, 2010, Proceedings, Part II*, volume 6441 of *Lecture Notes in Computer Science*, pages 537–544. Springer, 2010.

[217] J. Li, Y. Zhang, X. Chen, and Y. Xiang. Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers & Security*, 72:1–12, 2018.

[218] N. Li and Q. Wang. Beyond separation of duty: an algebra for specifying high-level security policies. In A. Juels, R. N. Wright, and S. D. C. di Vimercati, editors, *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 — November 3, 2006*, pages 356–369. ACM, 2006.

[219] Y. Li, N. Du, C. Liu, Y. Xie, W. Fan, Q. Li, J. Gao, and H. Sun. Reliable Medical Diagnosis from Crowdsourcing: Discover Trustworthy Answers from Non-Experts. In *WSDM'17: Proceedings of the tenth ACM international conference on web search and data mining*, pages 253–261. Assoc Comp Machinery; Assoc Comp Machinery Special Interest Grp Informat Retrieval; Assoc Comp Machinery SIGMOD; Assoc Comp Machinery SIGKDD; Assoc Comp Machinery SIGWEB, 2017. 10th ACM International Conference on Web Search and Data Mining (WSDM), Cambridge, ENGLAND, FEB 06-10, 2017.

[220] C. Liu, M. A. Ozols, M. Henderson, and A. Cant. A state-based model for certificate management systems. In *Public Key Cryptography, Third International Workshop on Practice and Theory in Public Key Cryptography, PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000, Proceedings*, pages 75–92, 2000.

[221] J. Liu, J. Tong, J. Mao, R. B. Bohn, J. V. Messina, M. L. Badger, and D. M. Leaf. *NIST Cloud Computing Reference Architecture*. National Institute of Standards and Technology, 2011.

[222] P. A. K. Lorimer, V. M.-F. Diec, and B. Kantarci. COVERS-UP: Collaborative Verification of Smart User Profiles for social sustainability of smart cities. *Sustainable Cities and Society*, 38:348–358, APR 2018.

[223] G. Lu, J. Lu, S. Yao, and J. Yip. A review on computational trust models for multi-agent systems. In *Proceedings of the 2007 International Conference on Internet Computing, ICOMP 2007, Las Vegas, Nevada, USA, June 25-28, 2007*, pages 325–331, 2007.

[224] N. Luhmann. *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexitaet*. Stuttgart: Ferdinand Enke, 1973.

[225] N. Luhmann. *Macht*. Stuttgart: Ferdinand Enke, 1975.

[226] N. Luhmann. *Trust and Power*. Chichester, Wiley, 1979.

[227] J. Lyle and A. Martin. Trusted Computing and Provenance: Better Together. In *Proceedings of the 2nd Workshop on the Theory and Practice of Provenance*. Usenix, 2010.

[228] M. Hepp. Goodrelations language reference V 1.0, Release 2011-10-01. http://www.heppnetz.de/ontologies/goodrelations/v1.html, 2011. Accessed: 2020-12-01.

[229] M. Sel, E. Üstündağ Soykan and E. Fasllija. Deliverable 2.5 on Trust and Trust Models. https://www.futuretrust.eu/deliverables, 2017. Accessed: 2020-06-20.

[230] M. Sel, G. Dißauer and T. Zefferer. Deliverable 2.6 Evaluation Scheme for Trustworthy Services. https://www.futuretrust.eu/deliverables, 2018. Accessed: 2020-06-23.

[231] K. Mahmud and M. Usman. Trust establishment and estimation in cloud services: A systematic literature review. *J. Network Syst. Manage.*, 27(2):489–540, 2019.

[232] E. Mansour, A. V. Sambra, S. Hawke, M. Zereba, S. Capadisli, A. Ghanem, A. Aboulnaga, and T. Berners-Lee. A demonstration of the solid platform for social web applications. In J. Bourdeau, J. Hendler, R. Nkambou, I. Horrocks, and B. Y. Zhao, editors, *Proceedings of the 25th International Conference on World Wide Web, WWW 2016, Montreal, Canada, April 11-15, 2016, Companion Volume*, pages 223–226. ACM, 2016.

[233] V. W. Marek and M. Truszczynski. Stable models and an alternative logic programming paradigm. In K. R. Apt, V. W. Marek, M. Truszczynski, and D. S. Warren, editors, *The Logic Programming Paradigm — A 25-Year Perspective*, Artificial Intelligence, pages 375–398. Springer, 1999.

[234] S. P. Marsh. *Formalising trust as a computational concept*. PhD thesis, University of Stirling, 1994. http://stephenmarsh.wdfiles.com/local--files/start/TrustThesis.pdf.

[235] A. Martin. The ten-page introduction to Trusted Computing. Technical Report RR-08-11, OUCL, December 2008. https://www.cs.ox.ac.uk/files/3449/PRG121.pdf.

[236] S. Mason. *Electronic Signatures in Law: Fourth Edition*. Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, 2016.

[237] S. Mason and M. C. Bromby. Response to digital agenda for Europe: Electronic identification, authentication and signatures in the European digital single market public consultation. *European Journal of Law and Technology*, 3(1), 2012.

[238] L. McKenna, C. Debruyne, and D. O'Sullivan. Modelling the Provenance of Linked Data Interlinks for the Library Domain. In *Companion of the World Wide Web conference (WWW 2019)*, pages 954–958. Assoc Comp Machinery; Microsoft; Amazon; Bloomberg; Google; Criteo AI Lab; CISCO; NTENT; Spotify; Yahoo Res; Wikimedia

Fdn; Baidu; DiDi; eBay; Facebook; LinkedIn; Megagon Labs; Mix; Mozilla; Netflix Res; NE Univ; Pinterest; Quora; Visa Res; Walmart Labs; Airbnb; Letgo; Moore Fdn; Webcastor, 2019. World Wide Web Conference (WWW), San Francisco, CA, MAY 13-17, 2019.

[239] P. M. Mell and T. Grance. *NIST Definition of Cloud Computing*. National Institute of Standards and Technology, 2011.

[240] E. Mendelson. *Introduction to mathematical logic (3. ed.)*. Chapman and Hall, 1987.

[241] A. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[242] X. Meng and D. Liu. Getrust: A guarantee-based trust model in chord-based p2p networks. *IEEE Transactions on Dependable and Secure Computing*, 15(01):54–68, jan 2018.

[243] C. Mitchell. Who needs trust for 5G? Workingpaper, arXiv, May 2020.

[244] R. M. Mohammad and H. Y. AbuMansour. An intelligent model for trustworthiness evaluation in semantic web applications. In *8th International Conference on Information and Communication Systems (ICICS)*, 2017.

[245] L. Moreau and P. T. Groth. *Provenance: An Introduction to PROV*. Synthesis Lectures on the Semantic Web: Theory and Technology. Morgan & Claypool Publishers, 2013.

[246] A. Moreno-Conde, G. Thienpont, I. Lamote, P. Coorevits, C. Parra, and D. Kalra. European Interoperability Assets Register and Quality Framework Implementation. In Hoerbst, A and Hackl, WO and DeKeizer, N and Prokosch, HU and HercigonjaSzekeres, M and DeLusignan, S, editor, *Exploring complexity in health: an interdisciplinary systems approach*, volume 228 of *Studies in Health Technology and Informatics*, pages 690–694, 2016. Medical Informatics Europe (MIE) Conference at Conference on Health - Exploring Complexity (HEC) - An Interdisciplinary Systems Approach, Munich, GERMANY, AUG 28-SEP 02, 2016.

[247] M. A. Morid, A. Omidvar, and H. R. Shahriari. An enhanced method for computation of similarity between the contexts in trust evaluation using weighted ontology. In *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, Changsha, China, 16-18 November, 2011*, pages 721–725. IEEE Computer Society, 2011.

[248] F. Moscato, B. D. Martino, and R. Aversa. Enabling model driven engineering of cloud services by using mosaic ontology. *Scalable Comput. Pract. Exp.*, 13(1), 2012.

[249] T. Muller, J. Zhang, and Y. Liu. A language for trust modelling. In J. Zhang, R. Cohen, and M. Sensoy, editors, *Proceedings of the 18th International Workshop on Trust in Agent Societies co-located with the 15th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2016), Singapore, Singapore, May 10, 2016.*, volume 1578 of *CEUR Workshop Proceedings*, pages 63–70. CEUR-WS.org, 2016.

[250] M. A. Musen. The Protégé project: a look back and a look forward. *AI Matters*, 1(4):4–12, 2015.

[251] C. S. Mustaffa and S. S. A. Baqi. Construction and Development of Quantitative Scale to Measure Source Credibility in the Maternal Mortality Context. *Pertanika Journal of Social Science and Humanities*, 24(1):53–96, MAR 2016.

[252] R. N. N. Hastings. Domain name system security extensions. RFC 5217, RFC Editor, July 2008. `http://www.rfc-editor.org/rfc/rfc5217.txt`.

[253] National Conference of Commisioners on Uniform State Laws. Uniform Electronic Transactions Act, 1999.

[254] National Institute of Standards and Technology. *Managing Information Security Risk. NIST Special Publication SP-800-39*, 2011. `https://csrc.nist.gov/publications/detail/sp/800-39/final`.

[255] National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems. NIST Special Publication SP-800-53 Rev.4*, 2013. `https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final`.

[256] D. M. Nessett. A critique of the Burrows, Abadi and Needham logic. *Operating Systems Review*, 24(2):35–38, 1990.

[257] NIST. *FIPS 180-1 Secure Hash Standard (SHS)*. National Institute of Standards and Technology, 1995.

[258] J. R. Nurse, I. Agrafiotis, M. Goldsmith, S. Creese, and K. Lamberts. Two sides of the coin: measuring and communicating the trustworthiness of online information. *Journal of Trust Management, https://journaloftrustmanagement.springeropen.com*, 2014.

[259] Oasis SAML Technical Committee. Security Assertion Markup Language. `https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security`.

[260] C. Okoli. A guide to conducting a standalone systematic literature review. *CAIS*, 37:43, 2015.

[261] A. Oltramari and J. Cho. ComTrustO: Composite trust-based ontology framework for information and decision fusion. In *18th International Conference on Information Fusion, FUSION 2015, Washington, DC, USA, July 6-9, 2015*, pages 542–549, 2015.

[262] A. Oltramari, L. F. Cranor, R. J. Walls, and P. D. McDaniel. Building an ontology of cyber security. In K. B. Laskey, I. Emmons, and P. C. G. Costa, editors, *Proceedings of the Ninth Conference on Semantic Technology for Intelligence, Defense, and Security, Fairfax VA, USA, November 18-21, 2014*, volume 1304 of *CEUR Workshop Proceedings*, pages 54–61. CEUR-WS.org, 2014.

[263] A. Oltramari, D. Piraviperumal, F. Schaub, S. Wilson, S. Cherivirala, T. B. Norton, N. C. Russell, P. Story, J. R. Reidenberg, and N. M. Sadeh. Privonto: A semantic framework for the analysis of privacy policies. *Semantic Web*, 9(2):185–203, 2018.

[264] M. O'Mara-Shimek. Levels of Ethical Quality of Metaphor in Stock Market Reporting. *Business and Society Review*, 122(1):93–117, SPR 2017.

[265] J. A. Onieva, J. Zhou, and J. López. Multiparty nonrepudiation: A survey. *ACM Comput. Surv.*, 41(1):5:1–5:43, 2008.

[266] Ontotext. *GraphDB Free Documentation Release 8.7*, 2018. Available from: `https://graphdb.ontotext.com/documentation/free/` (last accessed 15 December 2020).

[267] OpenID Foundation (OIDF). OpenID Connect Core 1.0 incorporating errata set 1. `https://openid.net/specs/openid-connect-core-1_0.html`.

[268] F. Osborne and E. Motta. Klink-2: Integrating multiple web sources to generate semantic topic networks. In *The Semantic Web — ISWC 2015 — 14th International Semantic Web Conference, Bethlehem, PA, USA, October 11-15, 2015, Proceedings, Part I*, pages 408–424, 2015.

[269] F. Osborne, E. Motta, and P. Mulholland. Exploring scholarly data with rexplore. In *The Semantic Web — ISWC 2013 — 12th International Semantic Web Conference, Sydney, NSW, Australia, October 21-25, 2013, Proceedings, Part I*, pages 460–477, 2013.

[270] N. Osman, P. Gutierrez, and C. Sierra. Trustworthy advice. *KNOWLEDGE-BASED SYSTEMS*, 82:41–59, JUL 2015.

[271] R. Perlman. An Overview of PKI Trust Models. *IEEE Network — November/December 1999*, 11 1999.

[272] G. Petrovic. *SoNeR FOAF dataset*, 2016. `https://data.mendeley.com/datasets/zp23s23xpb/1`.

[273] G. Petrovic and H. Fujita. SoNeR: Social network ranker. *Neurocomputing*, 202:104–107, 2016.

[274] K. R. POPPER. *The logic of scientific discovery.* Hutchinson, [3rd ed. (revised)].. edition, 1968.

[275] M. Qu, S. Liu, and T. Bao. On the trusted ontology model for evaluating the semantic web services. In W. Shen, N. Gu, T. Lu, J. A. Barthès, and J. Luo, editors, *Proceedings of the 2010 14th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2010, April 14-16, 2010, Fudan University, Shanghai, China*, pages 367–372. IEEE, 2010.

[276] S. Ries, S. M. Habib, M. Mühlhäuser, and V. Varadharajan. CertainLogic: A Logic for Modeling Trust and Uncertainty — (short paper). In *Trust and Trustworthy Computing — 4th International Conference, TRUST 2011, Pittsburgh, PA, USA, June 22-24, 2011. Proceedings*, pages 254–261, 2011.

[277] S. Ries and A. Heinemann. Analyzing the Robustness of CertainTrust. In Y. Karabulut, J. Mitchell, P. Herrmann, and C. D. Jensen, editors, *Trust Management II — Proceedings of IFIPTM 2008: Joint iTrust and PST Conferences on Privacy, Trust Management and Security, June 18-20, 2008, Trondheim, Norway*, volume 263 of *IFIP Advances in Information and Communication Technology*, pages 51–67. Springer, 2008.

[278] P. Ristoski and H. Paulheim. Semantic Web in data mining and knowledge discovery: A comprehensive survey. *J. Web Semant.*, 36:1–22, 2016.

[279] M. Rospocher, M. van Erp, P. Vossen, A. Fokkens, I. Aldabe, G. Rigau, A. Soroa, T. Ploeger, and T. Bogaard. Building event-centric knowledge graphs from news. *J. Web Semant.*, 37-38:132–151, 2016.

[280] J. I. C. Rubiera and J. M. M. López. A jade-based art-inspired ontology and protocols for handling trust and reputation. In *Ninth International Conference on Intelligent Systems Design and Applications, ISDA 2009, Pisa, Italy , November 30-December 2, 2009*, pages 300–305. IEEE Computer Society, 2009.

[281] S. Rudolph. Foundations of Description Logics. In A. Polleres, C. d'Amato, M. Arenas, S. Handschuh, P. Kroner, S. Ossowski, and P. F. Patel-Schneider, editors, *Reasoning Web. Semantic Technologies for the Web of Data — 7th International Summer School 2011, Galway, Ireland, August 23-27, 2011, Tutorial Lectures*, volume 6848 of *Lecture Notes in Computer Science*, pages 76–136. Springer, 2011.

[282] S. Rudolph. Foundations of description logics. In *Reasoning Web. Semantic Technologies for the Web of Data*, pages 76–136. Springer, 2011.

[283] S. Ruohomaa and L. Kutvonen. Trust management survey. In *Trust Management, Third International Conference, iTrust 2005, Paris, France, May 23-26, 2005, Proceedings*, pages 77–92, 2005.

[284] N. S. Safa, R. von Solms, and S. Furnell. Information security policy compliance model in organizations. *Computers & Security*, 56:70–82, 2016.

[285] A. A. Salatino, T. Thanapalasingam, A. Mannocci, F. Osborne, and E. Motta. The computer science ontology: A large-scale taxonomy of research areas. In *The Semantic Web — ISWC 2018 — 17th International Semantic Web Conference, Monterey, CA, USA, October 8-12, 2018, Proceedings, Part II*, pages 187–205, 2018.

[286] J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.

[287] A. V. Samsonvich. On semantic map as a key component in socially-emotional BICA. *Biologically Inspired Cognitive Architectures*, 23:1–6, Jan 2018.

[288] H. Schmidt. *National Strategy for Trusted Identities in Cyberspace*. The White House, 2011. `https://www.whitehouse.gov/` (accessed 1 November 2016).

[289] M. Schmidt-Schauß and G. Smolka. Attributive Concept Descriptions with Complements. *Artif. Intell.*, 48(1):1–26, 1991.

[290] F. B. Schneider and L. Zhou. Implementing trustworthy services using replicated state machines. *IEEE Security & Privacy*, 3(5):34–43, 2005.

[291] F. B. Schneider and L. Zhou. Implementing trustworthy services using replicated state machines. In *Replication: Theory and Practice*, pages 151–167, 2010.

[292] Secretary of State (UK). *Statutory Instrument 2016 No. 696 Electronic Communications*, 2016.

[293] Secretary of State (UK). *Statutory Instrument 2019 No. 89 Exiting the European Union Electronic Communications*, 2019.

[294] M. Sel. Using the semantic web to generate trust indicators. In S. Paulus, N. Pohlman, and H. Reimer, editors, *Securing Business Processes*, pages 106–119. Vieweg+Tuebner, Springer Science+Business Media, 2014.

[295] M. Sel. A comparison of trust models. In S. Paulus, N. Pohlman, and H. Reimer, editors, *Securing business processes*, pages 206–215. Vieweg+Tuebner, Springer Science+Business Media, 2015.

[296] M. Sel. Improving Interpretations of Trust Claims. In *Trust Management X — 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings*, pages 164–173, 2016.

[297] M. Sel, H. Diedrich, S. Demeester, and H. Stieber. *How smart contracts can implement "report once"*, 2017. Presented at the Data for Policy 2017: Government by Algorithm (Data for Policy), London: Zenodo https://doi.org/10.5281/zenodo.884497.

[298] M. Sel and D. Karaklajic. Internet of trucks and digital tachograph security and privacy threats. In S. Paulus, N. Pohlman, and H. Reimer, editors, *Securing Business Processes*, pages 230–238. Vieweg+Tuebner, Springer Science+Business Media, 2014.

[299] M. Sel and C. J. Mitchell. Automating the evaluation of trustworthiness. In *Proceedings of TrustBUS 2021: September 2021 (forthcoming). Springer-Verlag, 2021 (Lecture Notes in Computer Science)*, 2021.

[300] M. Sensoy, B. Yilmaz, and T. J. Norman. Stage: Stereotypical Trust Assessment Through Graph Extraction. *Computational Intelligence*, 32(1):72–101, FEB 2016.

[301] N. Shadbolt, T. Berners-Lee, and W. Hall. The semantic web revisited. *IEEE Intelligent Systems*, 21(3):96–101, 2006.

[302] S. Shekarpour and S. D. Katebi. Modeling and evaluation of trust with an extension in semantic web. *Web Semant.*, 8(1):26–36, Mar. 2010.

[303] W. Sherchan, S. Nepal, J. Hunklinger, and A. Bouguettaya. A trust ontology for semantic services. In *2010 IEEE International Conference on Services Computing, SCC 2010, Miami, Florida, USA, July 5-10, 2010*, pages 313–320. IEEE Computer Society, 2010.

[304] A. P. Sheth, B. Aleman-Meza, I. B. Arpinar, C. Bertram, Y. S. Warke, C. Ramakrishnan, C. Halaschek, K. Anyanwu, D. Avant, F. S. Arpinar, and K. Kochut. Semantic association identification and knowledge discovery for national security applications. *J. Database Manag.*, 16(1):33–53, 2005.

[305] I. Solodovnik and P. Budroni. Preserving digital heritage: At the crossroads of Trust and Linked Open Data. *IFLA Journal — International Federation of Library Associations*, 41(3, SI):251–264, OCT 2015.

[306] R. Steele and K. Min. Flexible wireless trust through ontology-based mapping and its attendant semantic limitations. In Y. Xiang, J. López, H. Wang, and W. Zhou, editors, *Third International Conference on Network and System Security, NSS 2009, Gold Coast, Queensland, Australia, October 19-21, 2009*, pages 240–245. IEEE Computer Society, 2009.

[307] K. Sullivan, J. Clarke, and B. P. Mulcahy. Trust-terms ontology for defining security requirements and metrics. In I. Gorton, C. E. Cuesta, and M. A. Babar, editors, *Software Architecture, 4th European Conference, ECSA 2010, Copenhagen, Denmark, August 23-26, 2010. Companion Volume*, ACM International Conference Proceeding Series, pages 175–180. ACM, 2010.

[308] M. Taheriyan, C. A. Knoblock, P. A. Szekely, and J. L. Ambite. Learning the semantics of structured data sources. *J. Web Semant.*, 37-38:152–169, 2016.

[309] H. J. ter Horst. Completeness, decidability and complexity of entailment for RDF schema and a semantic extension involving the OWL vocabulary. *J. Web Semant.*, 3(2-3):79–115, 2005.

[310] K. Thirunarayan and A. Sheth. Semantics-Empowered Big Data Processing with Applications. *AI Magazine*, 36(1):39–54, SPR 2015.

[311] J. Timpner, D. Schurmann, and L. Wolf. Trustworthy parking communities: Helping your neighbor to find a space. *IEEE Transactions on Dependable and Secure Computing*, 13(01):120–132, jan 2016.

[312] A. Tolk. Truth, trust, and turing — implications for modeling and simulation. In A. Tolk, editor, *Ontology, Epistemology, and Teleology for Modeling and Simulation — Philosophical Foundations for Intelligent M&S Applications*, volume 44 of *Intelligent Systems Reference Library*, pages 1–26. Springer, 2013.

[313] K. Toumi, C. Andrés, and A. R. Cavalli. Trust ontology based on access control parameters in multi-organization environments. In K. Yétongnon, A. Dipanda, and R. Chbeir, editors, *Ninth International Conference on Signal-Image Technology & Internet-Based Systems, SITIS 2013, Kyoto, Japan, December 2-5, 2013*, pages 285–292. IEEE Computer Society, 2013.

[314] T.-D. Trinh, P. R. Aryan, B.-L. Do, F. J. Ekaputra, E. Kiesling, A. Rauber, P. Wetz, and A. M. Tjoa. Linked Data Processing Provenance Towards Transparent and Reusable Linked Data Integration. In *2017 IEEE/WIC/ACM International Conference on Web*

Intelligence (WI 2017), pages 88–96. IEEE; WIC; ACM, 2017. IEEE/WIC/ACM International Conference on Web Intelligence (WI), Leipzig, GERMANY, AUG 23-26, 2017.

[315] N. Tsakalakis, S. Stalla-Bourdillon, and K. O'Hara. Identity assurance in the UK: technical implementation and legal implications under eIDAS. *The Journal of Web Science*, 3(3):32–46, December 2017.

[316] A. Tucker. *A two-person dilemma (unpublished, 1950, reprinted in 'Games and Information: An Introduction to Game Theory'*. Wiley-Blackwell, 2001.

[317] A. M. M. S. Ullah. Modeling and simulation of complex manufacturing phenomena using sensor signals from the perspective of Industry 4.0. *Advanced Engineering Informatics*, 39:1–13, Jan 2019.

[318] UNCITRAL. UNCITRAL Model Law on Electronic Commerce, 1996. `http://www.uncitral.org/uncitral/en/uncitral\_texts/electronic\_commerce/1996Model.html` Accessed: 2020-06-09.

[319] United States Office of Management and Budget (OMB). *Memorandum M-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors*, 2011.

[320] US Congress. *Public Law 106-229, An act to facilitate the use of electronic records and signatures in interstate or foreign commerce.*, 2000. `https://www.govinfo.gov/app/details/PLAW-106publ229`.

[321] US Congress. *Public Law 107-204 July 30, 2002 107th Congress — Sarbanes-Oxley Act*, 2002. `https://www.govinfo.gov/app/details/PLAW-107publ204`.

[322] US Department of Defense. *DoD Trusted Computer System Evaluation Criteria DOD 5200.28-STD*, 1985.

[323] M. Uschold. *Demystifying OWL for the Enterprise*. Synthesis Lectures on the Semantic Web: Theory and Technology. Morgan & Claypool Publishers, 2018.

[324] S. Van De Ven, R. Hoekstra, J. Breuker, L. Wortel, and A. El-Ali. Judging Amy: Automated legal assessment using OWL 2. In *OWLED*, volume 432, 2008.

[325] F. van Harmelen, V. Lifschitz, and B. W. Porter, editors. *Handbook of Knowledge Representation*, volume 3 of *Foundations of Artificial Intelligence*. Elsevier, 2008.

[326] S. VanRoekel. *Requirements for Accepting Externally-Issued Identity Credentials*. US Office of Management and Budget (OMB), 2011.

[327] R. Verborgh, M. V. Sande, O. Hartig, J. V. Herwegen, L. D. Vocht, B. D. Meester, G. Haesendonck, and P. Colpaert. Triple pattern fragments: A low-cost knowledge graph interface for the web. *J. Web Semant.*, 37-38:184–206, 2016.

[328] E. R. Verheul. The polymorphic eID scheme. Technical report, Ministry of Interior and Kingdom Relations The Hague The Netherlands, November 2019. `https://www.cs.ru.nl/E.Verheul/`.

[329] E. R. Verheul, B. Jacobs, C. Meijer, M. Hildebrandt, and J. de Ruiter. Polymorphic Encryption and Pseudonymisation for Personalised Healthcare. *IACR Cryptol. ePrint Arch.*, 2016:411, 2016.

[330] L. Viljanen. Towards an ontology of trust. In *Trust, Privacy and Security in Digital Business: Second International Conference, TrustBus 2005, Copenhagen, Denmark, August 22-26, 2005, Proceedings*, pages 175–184, 2005.

[331] J. vom Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, and A. Cleven. Reconstructing the giant: On the importance of rigour in documenting the literature search process. In *17th European Conference on Information Systems, ECIS 2009, Verona, Italy, 2009*, pages 2206–2217, 2009.

[332] V. G. V. Vydiswaran and M. Reddy. Identifying peer experts in online health forums. *BMC Medical Informatics and Decision Making*, 19(3), APR 4 2019.

[333] W3C. Resource Description Framework (RDF) Model and Syntax Specification — W3C Recommendation 22 February 1999. `https://www.w3.org/TR/1999/REC-rdf-syntax-19990222/`, 1999. Accessed: 2020-06-03.

[334] W3C. XML Path Language (Xpath) Version 1.0 W3C Recommendation 16 November 1999. `https://www.w3.org/TR/1999/REC-xpath-19991116/`, 1999. Accessed: 2020-12-09.

[335] W3C. OWL Web Ontology Language Overview. `https://www.w3.org/TR/2004/REC-owl-features-20040210/`, 2004. Accessed: 2020-06-04.

[336] W3C. RDF Concepts and Abstract Syntax. `https://www.w3.org/TR/2004/REC-rdf-concepts-20040210/`, 2004. Accessed: 2020-06-03.

[337] W3C. The RDF Primer. `https://www.w3.org/TR/2004/REC-rdf-primer-20040210/`, 2004. Accessed: 2020-06-03.

[338] W3C. RDF Semantics. https://www.w3.org/TR/2004/REC-rdf-mt-20040210/, 2004. Accessed: 2020-06-03.

[339] W3C. RDF Vocabulary Description Language 1.0: RDF Schema. https://www.w3.org/TR/2004/REC-rdf-schema-20040210/, 2004. Accessed: 2020-06-03.

[340] W3C. RDF/XML Syntax Specification (revised). https://www.w3.org/TR/2004/REC-rdf-syntax-grammar-20040210/, 2004. Accessed: 2020-06-03.

[341] W3C. The RDF Test Cases. https://www.w3.org/TR/2004/REC-rdf-testcases-20040210/, 2004. Accessed: 2020-06-03.

[342] W3C. OWL 2 Overview. https://www.w3.org/TR/2012/REC-owl2-overview-20121211/, 2012. Accessed: 2020-05-29.

[343] W3C. OWL 2 Web Ontology Language Conformance (Second Edition). https://www.w3.org/TR/2012/REC-owl2-conformance-20121211/, 2012. Accessed: 2020-05-29.

[344] W3C. OWL 2 Web Ontology Language Data Range Extension: Linear Equations (Second Edition). https://www.w3.org/TR/2012/NOTE-owl2-dr-linear-20121211/, 2012. Accessed: 2020-05-29.

[345] W3C. OWL 2 Web Ontology Language Data Range Extension: Linear Equations (Second Edition). https://www.w3.org/TeamSubmission/turtle/, 2012. Accessed: 2020-05-29.

[346] W3C. OWL 2 Web Ontology Language Direct Semantics (Second Edition). https://www.w3.org/TR/2012/REC-owl2-direct-semantics-20121211/, 2012. Accessed: 2020-05-29.

[347] W3C. OWL 2 Web Ontology Language Manchester Syntax (Second Edition). https://www.w3.org/TR/2012/NOTE-owl2-manchester-syntax-20121211/, 2012. Accessed: 2020-05-29.

[348] W3C. OWL 2 Web Ontology Language Mapping to RDF Graphs (Second Edition). https://www.w3.org/TR/2012/REC-owl2-mapping-to-rdf-20121211/, 2012. Accessed: 2020-05-29.

[349] W3C. OWL 2 Web Ontology Language Primer (Second Edition). https://www.w3.org/TR/owl2-primer/, 2012. Accessed: 2020-05-29.

[350] W3C. OWL 2 Web Ontology Language Profiles (Second Edition). https://www.w3.org/TR/2012/REC-owl2-profiles-20121211/, 2012. Accessed: 2020-05-29.

[351] W3C. OWL 2 Web Ontology Language RDF-Based Semantics (Second Edition). https://www.w3.org/TR/2012/REC-owl2-rdf-based-semantics-20121211/, 2012. Accessed: 2020-05-29.

[352] W3C. OWL 2 Web Ontology Language Structural Specification and Functional-Style Syntax (Second Edition). https://www.w3.org/TR/2012/REC-owl2-syntax-20121211/, 2012. Accessed: 2020-05-29.

[353] W3C. OWL 2 Web Ontology Language XML Serialization (Second Edition). https://www.w3.org/TR/2012/REC-owl2-xml-serialization-20121211/, 2012. Accessed: 2020-05-29.

[354] W3C. Constraints of the PROV Data Model W3C Recommendation 30 april 2013. https://www.w3.org/TR/2013/REC-prov-constraints-20130430/, 2013. Accessed: 2020-12-01.

[355] W3C. PROV-DM: The PROV Data Model W3C recommendation 30 April 2013. https://www.w3.org/TR/prov-dm/, 2013. Accessed: 2020-12-01.

[356] W3C. PROV-N: The Provenance Notation W3C Recommendation 30 April 2013. https://www.w3.org/TR/2013/REC-prov-n-20130430/, 2013. Accessed: 2020-12-01.

[357] W3C. PROV-O: The PROV Ontology W3C Recommendation 30 April 2013. https://www.w3.org/TR/prov-o/, 2013. Accessed: 2020-12-01.

[358] W3C. RDF 1.1 Concepts and Abstract Syntax. https://www.w3.org/TR/2014/REC-rdf11-concepts-20140225/, 2014. Accessed: 2020-05-27.

[359] W3C. RDF 1.1 Primer. https://www.w3.org/TR/2014/NOTE-rdf11-primer-20140624/, 2014. Accessed: 2020-05-27.

[360] W3C. RDF 1.1 Schema. https://www.w3.org/TR/rdf-schema/, 2014. Accessed: 2020-05-27.

[361] W3C. RDF 1.1 Semantics. https://www.w3.org/TR/2014/REC-rdf11-mt-20140225/, 2014. Accessed: 2020-05-27.

[362] W3C. RDF 1.1 Test Cases. https://www.w3.org/TR/2014/NOTE-rdf11-testcases-20140225/, 2014. Accessed: 2020-05-27.

[363] W3C. RDF 1.1 XML Syntax. https://www.w3.org/TR/rdf-syntax-grammar/, 2014. Accessed: 2020-05-27.

[364] W3C. SPARQL 1.1 Entailment. https://www.w3.org/TR/sparql11-entailment/, 2014. Accessed: 2020-05-27.

[365] W3C. SPARQL 1.1 Federated Query. https://www.w3.org/TR/sparql11-federated-query/, 2014. Accessed: 2020-05-28.

[366] W3C. SPARQL 1.1 Graph Store HTTP Protocol. https://www.w3.org/TR/sparql11-http-rdf-update/, 2014. Accessed: 2020-05-28.

[367] W3C. SPARQL 1.1 Overview. https://www.w3.org/TR/sparql11-overview/, 2014. Accessed: 2020-05-28.

[368] W3C. SPARQL 1.1 Protocol for RDF. https://www.w3.org/TR/sparql11-protocol/, 2014. Accessed: 2020-05-28.

[369] W3C. SPARQL 1.1 Query Language. https://www.w3.org/TR/sparql11-query/, 2014. Accessed: 2020-05-28.

[370] W3C. SPARQL 1.1 Query Results CSV and TSV formats. https://www.w3.org/TR/sparql11-results-csv-tsv/, 2014. Accessed: 2020-05-28.

[371] W3C. SPARQL 1.1 Query Results JSON format. https://www.w3.org/TR/sparql11-results-json/, 2014. Accessed: 2020-05-28.

[372] W3C. SPARQL 1.1 Query Results XML formats. https://www.w3.org/TR/sparql11-overview/\#SPARQL-XML-Result, 2014. Accessed: 2020-05-28.

[373] W3C. SPARQL 1.1 Service Description. https://www.w3.org/TR/sparql11-service-description/, 2014. Accessed: 2020-05-28.

[374] W3C. SPARQL 1.1 Test Cases. https://www.w3.org/2009/sparql/docs/tests/, 2014. Accessed: 2020-05-28.

[375] W3C. SPARQL 1.1 Update Language. https://www.w3.org/TR/sparql11-update/, 2014. Accessed: 2020-05-28.

[376] W3C. The Organization Ontology W3C Recommendation 16 january 2014. https://www.w3.org/TR/vocab-org/, 2014. Accessed: 2020-12-01.

[377] W3C. XSL Transformations (XSLT) Version 3.0 W3C Recommendation 8 June 2017. https://www.w3.org/TR/xslt-30/, 2017. Accessed: 2020-12-09.

[378] W3C. Verifiable Credentials Data Model 1.0. https://www.w3.org/TR/vc-data-model/, 2019. Accessed: 2021-01-05.

[379] W3C. Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/, 2021. Accessed: 2021-01-05.

[380] R. Wang, D. Sun, G. Li, M. Atif, and S. Nepal. LogProv: Logging Events as Provenance of Big Data Analytics Pipelines with Trustworthiness. In Joshi, J and Karypis, G and Liu, L and Hu, X and Ak, R and Xia, Y and Xu, W and Sato, AH and Rachuri, S and Ungar, L and Yu, PS and Govindaraju, R and Suzumura, T, editor, *2016 IEEE International Conference on Big Data (BIG DATA)*, pages 1402–1411. IEEE; IEEE Comp Soc; Natl Sci Fdn; Cisco; Huawei; Elsevier; Navigant; Johns Hopkins Whiting Sch Engn, 2016. 4th IEEE International Conference on Big Data (Big Data), Washington, DC, DEC 05-08, 2016.

[381] Y. Wang, G. Yin, Z. Cai, Y. Dong, and H. Dong. A trust-based probabilistic recommendation model for social networks. *J. Network and Computer Applications*, 55:59–67, 2015.

[382] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. A. Hendler, and G. J. Sussman. Information accountability. *Commun. ACM*, 51(6):82–87, 2008.

[383] J. Werbrouck, P. Pauwels, J. Beetz, and L. van Berlo. Towards a decentralised common data environment using linked building data and the solid ecosystem. In B. Kumar, F. Rahimian, D. Greenwood, and T. Hartmann, editors, *Advances in ICT in Design, Construction and Management in Architecture, Engineering, Construction and Operations (AECO) : Proceedings of the 36th CIB W78 2019 Conference*, pages 113–123, 2019.

[384] J. Wielemaker, M. Hildebrand, and J. van Ossenbruggen. Prolog as the fundament for applications on the semantic web. In A. Polleres, D. Pearce, S. Heymans, and E. Ruckhaus, editors, *Proceedings of the ICLP'07 Workshop on Applications of Logic Programming to the Web, Semantic Web and Semantic Web Services, ALPSWS 2007, Porto, Portugal, September 13th, 2007*, volume 287 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2007.

[385] P. Wongthongtham and B. Abu-Salih. Ontology and trust based data warehouse in new generation of business intelligence: State-of-the-art, challenges, and opportunities. In *13th IEEE International Conference on Industrial Informatics, INDIN 2015, Cambridge, United Kingdom, July 22-24, 2015*, pages 476–483. IEEE, 2015.

[386] H. Zhang, Y. Li, F. Ma, J. Gao, and L. Su. TextTruth: An Unsupervised Approach to Discover Trustworthy Information from Multi-Sourced Text Data. In *KDD'18: Proceedings of the 24TH ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, pages 2729–2737. Assoc Comp Machinery; Assoc Comp Machinery SIGKDD; Assoc Comp Machinery SIGMOD, 2018. 24th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD), London, England, AUG 19-23, 2018.

[387] N. Zhang and Q. Shi. Achieving non-repudiation of receipt. *Comput. J.*, 39(10):844–853, 1996.

[388] Y. Zhang, B. Fang, and C. Xu. Preference ontology-oriented metric model for trustworthy web services. *Int. J. Intell. Syst.*, 26(2):158–168, 2011.

[389] Y. Zhong, B. Bhargava, Y. Lu, and P. Angin. A computational dynamic trust model for user authorization. *IEEE Transactions on Dependable and Secure Computing*, 12(01):1–15, jan 2015.

[390] J. Zhou and D. Gollmann. Observations on non-repudiation. In K. Kim and T. Matsumoto, editors, *Advances in Cryptology — ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3-7, 1996, Proceedings*, volume 1163 of *Lecture Notes in Computer Science*, pages 133–144. Springer, 1996.

[391] C. Zhu and X. Dai. Model of trust management based on finite state machine. In *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012, Kuala Lumpur, Malaysia, June 26-28, 2012*, pages 161–164. IEEE, 2012.

[392] M. Zhu and Z. Jin. Trust analysis of web services based on a trust ontology. In Z. Zhang and J. H. Siekmann, editors, *Knowledge Science, Engineering and Management, Second International Conference, KSEM 2007, Melbourne, Australia, November 28-30, 2007, Proceedings*, volume 4798 of *Lecture Notes in Computer Science*, pages 642–648. Springer, 2007.

Part IV

Appendices

Appendix A

Survey

This appendix provides additional information on the literature survey described in Chapter 3.

A.1 Background information

A.1.1 Google Scholar

A search in Google Scholar for trust or trustworthiness returns millions of results. The search engine's user interface allows querying through search terms and natural language. It uses underlying structures which are not made public. Hence it is treated here as using a natural language vocabulary.

The selection that Google Scholar makes is not transparent. It ranks the search results and shows only the first 1,000 results of any search, based on algorithms that Google changes at their discretion. The ranking depends on settings such as language settings or location.

Google Scholar does not offer guidance on search terminology to use except for a basic description of search tips. These address how to limit the search period, how to obtain the full text, and how to use references found inside articles as pointers. Nevertheless as the tool covers a wide range of academic sources, a search was conducted. The following results were obtained on 29 May 2019.

- The results shown in Table A.1 were obtained by using the query terms that are shown in the first column, which always include the term 'trust'.
- The results shown in Table A.2 were obtained by using the query terms that are shown in the first column, which always include the term 'trustworthiness'.

Candidate terms returned from the query *semantic models of trust* in the period 2009-2019 were evaluation of trust, social trust ensemble, trust and distrust, and computational trust mod-

Google Scholar - query terms including trust	Period	Number of results
trust	Not specified	about 3,700,000 results
trust	2009-2019	about 1,690,000 results
meaning of trust	Not specified	about 3,120,000 results
meaning of trust	2009-2019	about 1,450,000 results
trust electronic society	Not specified	about 2,000,000 results
trust electronic society	2009-2019	about 430,000 results
meaning of trust in electronic society	Not specified	about 1,010,000 results
meaning of trust in electronic society	2009-2019	about 152,000 results
semantics of trust	Not specified	about 255,000 results
semantics of trust	2009-2019	about 50,600 results
semantic models of trust	Not specified	about 367,000 results
semantic models of trust	2009-2019	about 97,900 results
semantic models of trust	since 2018	about 17,400 results

Table A.1: Google Scholar table (trust)

els. Limiting the terms to results since 2018 yielded semantic trust model, framework to support trust, flow of trust with semantic web technologies, trust attributes, trust and liking rate, and methods for identifying fake news.

Candidate terms from the query *semantic models of trustworthiness* in the period 2009-2019 were provably trustworthy hardware, fuzzy reputation logic, trustworthiness at runtime, ontologies for trustworthy solutions, and trustworthy components. Limiting the terms to results since 2018 yielded trustworthy systems development, API trustworthiness, ontology based reasoning about trustworthiness, trustworthy, responsible, interpretable system and trustworthiness measurement from knowledge graph.

A.1.2 Microsoft Academic

A search on Microsoft Academic returned thousands of results. Searching can be done by author, author's institution, paper's publication title, journal, topic and conference. The search engine is not transparent about the classification algorithms. Nevertheless as the tool covers a wide range of academic sources, searches including trustworthiness were conducted. The results that are shown in Table A.3 were obtained on 3 June 2019.

Microsoft Academic did not allow to select beyond 2018. The results were broad and included many references to social sciences and chemistry. Candidate search terms identified from 'semantics of trustworthiness' were attestation, evidence, trustworthy fulfilment of commitments, subjective logic, uncertainty, provenance and sentiment.

Google Scholar - query term including trustworthiness	**Period**	**Number of results**
trustworthiness	Not specified	about 378,000 results
trustworthiness	2009-2019	about 93,900 results
meaning of trustworthiness	Not specified	about 193,000 results
meaning of trustworthiness	2009-2019	about 53,200 results
trustworthiness electronic society	Not specified	about 88,200 results
trustworthiness electronic society	2009-2019	about 22,300 results
meaning of trustworthiness in electronic society	Not specified	about 91,600 results
meaning of trustworthiness in electronic society	2009-2019	about 17,800 results
semantics of trustworthiness	Not specified	about 30,000 results
semantics of trustworthiness	2009-2019	about 16,100 results
semantic models of trustworthiness	Not specified	about 61,800 results
semantic models of trustworthiness	2009-2019	about 17,600 results
semantic models of trustworthiness	since 2018	about 13,300 results

Table A.2: Google Scholar table (trustworthiness)

Microsoft Academic - query term including trustworthiness	Period	Number of results
trustworthiness	2008-2018	5000+ results
meaning of trustworthiness	2008-2018	42 results
trustworthiness electronic society	2008-2018	407 results
meaning of trustworthiness in electronic society	2008-2018	447 results
semantics of trustworthiness	2008-2018	56 results

Table A.3: Microsoft Academic table (trustworthiness)

A.1.3 Possible terms

Taking into consideration the envisaged scope for the review, the following terms were identified from the above unstructured sources (in alphabetical order): attestation, API trustworthiness, computational trust models, evaluation of trust, evidence, flow of trust with semantic web technologies, interpretable system, ontology based reasoning about trustworthiness, ontologies for trustworthy solutions, provenance, semantic trust model, trust attributes, trustworthy fulfilment of commitments and trustworthiness measurement from knowledge graph.

A.1.4 Structured terms

Information providers using structured terms include the Web of Science (WOS), the 2012 ACM CCS Classification, the IEEE taxonomy, and the Computer Science Ontology.

The WOS covers journals, books and conference proceedings in its Core Collection. These are produced by commercial or open access publishers, and categorised and indexed by Clarivate Analytics. They make use of keywords, 252 subject categories mapped to 151 broadly defined research areas, including Engineering, Chemistry, Computer Science, Physics, and Mathematics. No keywords, categories or research areas are directly related to trust or trustworthiness.

The 2012 ACM Computing Classification System has been developed as a poly-hierarchical ontology, integrated into the search capabilities and topic displays of the ACM Digital Library. A search at the top level for the term trustworthiness did yield no results (29/5/2019). A search in the on-line ACM CCS at the top level for the term trust yielded four results (29/5/2019):

- information systems/world wide wide/web applications/crowdsourcing/trust
- security and privacy/formal methods and theory of security/ trust frameworks
- security and privacy/systems security/operating systems security/mobile platform security/trusted computing

- social and professional topics/computing technology policy/commerce policy/antitrust and competition

A search at the top level for the term semantics yielded the following results (29/5/2019):

- Software notations and tools/General programming languages/Formal language definitions/Semantics
- Theory Of Computation/Semantics and reasoning/Program semantics/
  - Algebraic semantics
  - Denotational semantics
  - Operational semantics
  - Axiomatic semantics
  - Action semantics
  - Categorical semantics
- Computing Methodologies/Symbolic and algebraic manipulation/Artificial intelligence/-Natural language processing/Lexical semantics
- Computing Methodologies/Symbolic and algebraic manipulation/Artificial intelligence/-Knowledge representation and reasoning/Semantic networks
- Information Systems/Information Systems Applications/World Wide Web/Web data description languages/Semantic web description languages

The IEEE publishes the IEEE Taxonomy, which comprises the first three hierarchical levels under each term-family (or branch) that is formed from the top-most terms of the IEEE Thesaurus. The latter is a controlled vocabulary of about 10,100 descriptive engineering, technical, and scientific terms as well as IEEE-specific society terms. The taxonomy did not yield any useful search terms. No matches were found for trustworthiness. The results are given in Table A.4.

The Computer Science Ontology (CSO) [285] is a large-scale ontology of research areas that was automatically generated using the Klink-2 algorithm [268] on the Rexplore dataset [269], which consists of about 16 million publications, mainly in the field of Computer Science. The Klink-2 algorithm combines semantic technologies, machine learning, and knowledge from external sources to automatically generate an ontology of research areas. Some relationships were also revised manually by experts during the preparation of two ontology-assisted surveys in the field of Semantic Web and Software Architecture. The main root of CSO is Computer Science,

Term	Related term	Broader or narrower term
Semantics	natural language processing, communication	broader term of semantic search, of semantic technology, of semiotics
Trust management	access control, computer security, cryptography, privacy	narrower term to decision making, to information security

Table A.4: IEEE thesaurus terms

however, the ontology includes also a few secondary roots, such as Linguistics, Geometry, and Semantics. A search on 13 June 2019 for 'semantics' returned 13 results, described in Table A.5. Regarding 'semantics of trust' and 'semantics of trustworthiness' no matching CSO concept were identified.

A.1.4.1 Summary of identified candidate search terms from structured sources

The following candidate terms were identified from the above structured sources: trust frameworks, trusted computing, denotational semantics, semantic web description languages, argumentation semantics.

A.1.4.2 Selected terminology and search terms

The following selection criteria were applied to select the initial search terms. The search terms must have the potential to lead to search results that are related to semantics, meaning, automation or logic. Those terms that lead to reputation systems, belief, subjective opinions, statistics and probability are not included. On this basis, subjective logic is not withheld as a search term, because it a type of probabilistic logic. Following terms were identified from the above sources:

- from the unstructured sources:
    - semantic trust model,
    - evaluation of trust,
    - computational trust models,

Term	Description (extract)
semantics	-
operational semantics	Operational semantics are a category of formal programming language semantics in which certain desired properties of a program, such as correctness, safety or security, are verified.
denotational semantics	In computer science, denotational semantics (initially known as mathematical semantics or Scott–Strachey semantics) is an approach of formalizing the meanings of programming languages.
lexical semantics	Lexical semantics (also known as lexicosemantics), is a subfield of linguistic semantics. The units of analysis in lexical semantics are lexical units which include not only words but also sub-words.
image semantics	-
argumentation semantics	Argumentation theory, or argumentation, is the interdisciplinary study of how conclusions can be reached through logical reasoning; that is, claims based, soundly or not, on premises.
well founded semantics	-
answer set semantics	-
structural operational semantics	Operational semantics are a category of formal programming language semantics in which certain desired properties of a program, such as correctness, safety or security, are verified.
formal semantics	In logic, the semantics of logic is the study of the semantics, or interpretations, of formal and (idealizations of) natural languages usually trying to capture the pre-theoretic notion of entailment.
Kripke semantics	Kripke semantics (also known as relational semantics or frame semantics, and often confused with possible world semantics) is a formal semantics for non-classical logic systems created in the late 1950s.
stable model semantics	The concept of a stable model, or answer set, is used to define a declarative semantics for logic programs with negation as failure.

Table A.5: CSO terms

- ontology based reasoning about trustworthiness,
- ontologies for trustworthy solutions,
- trustworthy fulfilment of commitments,
- trustworthiness measurement from knowledge graph,

- from the structured sources:
  - trusted computing,
  - denotational semantics,
  - argumentation semantics.

A.1.5 Sources

The identification of candidate sources was based on interaction with my supervisor, a study of the Royal Holloway University of London's Information Security Group training material on the topic, a review of trust related and semantic web related conference proceedings (IFIP TM, DEXA/TrustBus, ISWC) and on-line research. Candidate sources were identified in two tiers. The first tier consisted of providers that make citation indexing and ranking a core part of their offering.

- WOS (Clarivate Analytics, citation index),
- CiteseerX (Pennsylvania State University, automated citation indexing and digital library),
- Scopus (Elsevier, citation index),
- ScienceDirect (Elsevier, citation index),
- Google Scholar.

The second tier consisted of providers that focus on offering access to information repositories. This includes libraries, search engines and publishers.

- ZETOC (British Library's Electronic Table of Contents),
- Archives such as arXiv (Cornell University) and IACR (Cryptology ePrint archive),
- DBLP (database and logic programming bibliography site, University of Trier),
- Semantic Scholar (AI-backed search engine for scientific journal articles, the Allen Institute),

- Professional bodies such as ACM (Association for Computing Machinery) and IEEE (Institute of Electrical and Electronics Engineers) ,
- Commercial publishers such as Elsevier, Taylor and Francis, IOS Press, Springer,
- Oxford Journals (related to Computer Science),
- IOS Press(independent publishing house established in 1987 in Amsterdam),
- Open Access such as Zenodo from CERN,
- Technology providers such as Microsoft Academic Research and IBM Research.

Appendix B

Longlist

This appendix contains the longlist of articles considered for the literature review described in Chapter 3. The articles are listed per source.

B.1 WOS

A WOS basic search for 'semantic model of trustworthiness' was performed, using WOS Core Collection, searching in SCIE, from 2014 to present. This search returned 25 results.

1. Identifying peer experts in online health forums, Vydiswaran, V. G. Vinod and Reddy, Manoj, BMC Medical Informatics and Decision Making, 2019, [332],
2. Modelling the Provenance of Linked Data Interlinks for the Library Domain, McKenna, L. et al. , Companion of the World Wide Web Conference (WWW 2019), [238]
3. Modeling and simulation of complex manufacturing phenomena using sensor signals from the perspective of Industry 4.0, Ullah, A. M. M. Sharif, Advanced Engineering Informatics (journal), 2019, [317],
4. A generalized stereotype learning approach and its instantiation in trust modeling, Fang, Hui et al. , Electronic Commerce Research and Applications (journal), 2018, [113],
5. COVERS-UP: Collaborative Verification of Smart User Profiles for social sustainability of smart cities, Lorimer, Philip A. K. et al. , Sustainable Cities and Society (journal), 2018, [222],
6. TextTruth: An Unsupervised Approach to Discover Trustworthy Information from Multi-Sourced Text Data, Zhang, Hengtong et al. , KDD'18: Proceedings of the 24TH ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2018, [386],

7. Data trustworthiness and user reputation as indicators of VGI quality, Fogliaroni, Paolo et al. , Geo-spatial Information Science (journal), 2018, [117],

8. On semantic map as a key component in socially-emotional BICA, Samsonvich, Alexei V., Biologically Inspired Cognitive Architectures (journal), 2018, [287],

9. Levels of Ethical Quality of Metaphor in Stock Market Reporting, O'Mara-Shimek, M., Business and Society Review (journal), 2018, [264],

10. Linked Data Processing Provenance Towards Transparent and Reusable Linked Data Integration, Trinh, Tuan-Dat et al. , IEEE/WIC/ACM International Conference on Web Intelligence, Leipzig, Germany, 2017, [314],

11. An Intelligent Model for Trustworthiness Evaluation in Semantic Web Applications, Mohammad, Rami M. and AbuMansour, Hussein Y., 8th International Conference on Information and Communication Systems, 2017, [244],

12. An Ontology Based Trust Framework for Sensor-Driven Pervasive Environment, Karthik, N. and Ananthanarayana, V. S. , Asia Modelling Symposium AMS, 2017, [197],

13. Reliable Medical Diagnosis from Crowdsourcing: Discover Trustworthy Answers from Non-Experts, Li, Yaliang et al. , 10th ACM International Conference on Web Search and Data Mining (WSDM), Cambridge, England, 2017, [219],

14. DISARM: A social distributed agent reputation model based on defeasible logic, Kravari, K. and Bassiliades, N., Journal of Systems and Software, 2016, [204],

15. Construction and Development of Quantitative Scale to Measure Source Credibility in the Maternal Mortality Context, Mustaffa, Che Su and Baqi, Salah Saudat Abdul, Pertanika Journal of Social Science and Humanities, 2016, [251],

16. Stage: Stereotypical Trust Assessment Through Graph Extraction, Sensoy, Murat et al. , Journal of Computational Intelligence, 2016, [300],

17. LogProv: Logging Events as Provenance of Big Data Analytics Pipelines with Trustworthiness, Wang, Ruoyu et al. , 2016 IEEE International Conference on Big Data, [380],

18. European Interoperability Assets Register and Quality Framework Implementation, Moreno-Conde, Alberto et al. , Studies in Health Technology and Informatics, 2016, [246],

19. Formal Methods for a System of Systems Analysis Framework Applied to Traffic Management, Dickerson, Charles E. et al. , 11th IEEE System of Systems Engineering Conference (SoSE), Kongsberg, Norway, 2016, [71],

20. Preserving digital heritage: At the crossroads of Trust and Linked Open Data, Solodovnik, Iryna et al. , IFLA Journal International Federation of Library Association, 2015, [305],

21. Intercloud Trust and Security Decision Support System: an Ontology-based Approach, Bernal Bernabe et al. , Journal of Grid Computing, 2015, [27],

22. Trustworthy advice, Osman, Nardine et al. , Journal of Knowledge Based Systems, 2015, [270],

23. Trustworthy Service Discovery for Dynamic Web Service Composition, Kim, Yukyong et al. , KSII Transactions on Internet and Information Systems, 2015, [200],

24. Semantics-Empowered Big Data Processing with Applications, Thirunarayan, Krishnaprasad et al. , AI Magazine, 2015, [310],

25. Energy Consumption Analysis Method of CPS Software Based on Architecture Modeling, Hou Gang et al. , 9th International Conference on Frontier of Computer Science and Technology, Dalian, Peoples Republic of China, 2015, [120].

B.2 IEEE

A query for articles (2/8/2019) in IEEE Transactions on Dependable and Secure Computing (TDSC) on *'semantic model of trustworthiness'* in the period 2014-2019 yielded 110 results. Based on relevance the following 5 articles were selected.

1. A Computational Dynamic Trust Model for User Authorization, Yuhui Zhong et al. , IEEE Transactions on Dependable and Secure Computing, 2015, [389],

2. PROVEST: Provenance-Based Trust Model for Delay Tolerant Networks, Cho and Chen, IEEE Transactions on Dependable and Secure Computing, 2018, [58],

3. GeTrust: A Guarantee-Based Trust Model in Chord-Based P2P Networks, Xianfu Meng et al. , IEEE Transactions on Dependable and Secure Computing, 2018, [242],

4. Trust-Based Service Management for Social Internet of Things, Chen et al. , IEEE Transactions on Dependable and Secure Computing, 2016, [55],

5. Trustworthy Parking Communities: Helping Your Neighbor to Find a Space, Timpner J. et al. , IEEE Transactions on Dependable and Secure Computing, 2016, [311],

B.3 TrustBus and IFIP TM conference proceedings

A dedicated search of conference proceedings from TrustBus and IFIP TM conferences (including their references) was performed. 49 articles were identified.

1. A Calculus for Trust and Reputation Systems, Aldini A., Trust Management VIII - 8th IFIP WG 11.11 International Conference, IFIPTM 2014, Singapore, July 7-10, 2014, Proceedings, [4],

2. Basic concepts and taxonomy of dependable and secure computing, Avizienis et al. , Journal IEEE Trans. Dependable Sec. Comput., 2004, [13],

3. M-STAR: A Modular, Evidence-based Software Trustworthiness Framework, Alexopoulos et al. , CoRR, 2018, [5],

4. How Human Trusters Assess Trustworthiness in Quasi-virtual Contexts, Bacharach M., Trust, Reputation, and Security: Theories and Practice, AAMAS 2002 International Workshop, Bologna, Italy, 2002, Selected and Invited Papers, [17],

5. Challenges for Trusted Computing, S. Balfe et al. , IEEE Security and Privacy Magazine 2008, [20],

6. Authentication: A Practical Study in Belief and Action, Burrows M. et al. , Proceedings of the 2nd Conference on Theoretical Aspects of Reasoning about Knowledge, Pacific Grove, CA, USA, March 1988, [38],

7. Named graphs, provenance and trust, Jeremy J. Carroll, Proceedings of the 14th international conference on World Wide Web, 2005, Chiba, Japan, [45],

8. A trust model for data sharing in smart cities, Cao QH, et al. , IEEE International Conference on Communications 2016, [43],

9. Building general purpose security services on trusted computing, Chunhua Chen et al. , Trusted Systems: Third International Conference, INTRUST 2011, Beijing, China, November 27-29, 2011, Revised Selected Papers, [54],

10. Towards the Definition of an Ontology for Trust in (Web) Data, Ceolin D. et al. , Proceedings of the 10th International Workshop on Uncertainty Reasoning for the Semantic Web (URSW 2014), [51],

11. Bridging Gaps Between Subjective Logic and Semantic Web, Ceolin D. et al. , Uncertainty Reasoning for the Semantic Web III - ISWC International Workshops, URSW 2011-2013, Revised Selected Papers, [49],

12. Calculating the Trust of Event Descriptions using Provenance, Ceolin D., Proceedings of the Second International Workshop on the role of Semantic Web in Provenance Management, ISWC 2010, Shanghai, China, [48],

13. Trustworthy Systems Design using Semantic Risk Modelling, Ajay Chakravarthy et al. , Proceedings of the TrustBus 2012 Conference, [53],

14. A novel trust management framework for multi-cloud environments based on trust service providers, Wenjuan Fan and Harry G. Perros, Journal Knowl.-Based Syst., 2014, [112],

15. Mathematical Modelling of Trust Issues in Federated Identity Management, Md. Sadek Ferdous et al. 9th IFIP WG 11.11 International Conference, IFIPTM 2015, Hamburg, Germany, [116],

16. A formal notion of trust –enabling reasoning about security properties, Fuchs, Gürgens and Rudolph, IFIP TM 2010 conference proceedings, [118],

17. Towards content trust of web resources, Gil Y. and Artz D., Journal of Web Semantics, 2007, [121],

18. Trust Networks on the Semantic Web, Golbeck J. et al. Cooperative Information Agents VII, 7th International Workshop, CIA 2003, Helsinki, Finland, [128],

19. Computational trust methods for security quantification in the cloud ecosystem, Habib et al. The Cloud Security Ecosystem - Technical, Legal, Business and Management Issues, 2015, [140],

20. Trust4App: Automating Trustworthiness Assessment of Mobile Applications, Habib et al. 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering, TrustCom/BigDataSE 2018, NY, USA, 2018, [138],

21. Data-Purpose Algebra: Modeling Data Usage Policies, Hanson C. et al. proceedings of the 8th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2007), [142],

22. Querying Trust in RDF data with tSPARQL, Hartig O., ESWC 2009 conference proceeding, [143],

23. The hoonoh ontology for describing trust relationships in information seeking, Heath, T. and Motta, E., Personal Identification and Collaborations: Knowledge Mediation and Extraction (PICKME2008), [145],

24. Modelling Trust Structures for Public Key Infrastructures, Henderson M. et al. Information Security and Privacy, 7th Australian Conference, ACISP Melbourne, Australia, 2002, [146],

25. A calculus of Trust and its application to PKI and identity management, Huang and Nicol, ACM IDTrust 2009 conference proceeding, [157],

26. An ontology of trust: formal semantics and transitivity, Jingwei Huang and Mark S. Fox, The new e-commerce - Innovations for Conquering Current Barriers, Obstacles and Limitations to Conducting Successful Business on the Internet, 2006, Fredericton, New Brunswick, Canada, [155],

27. A calculus of Trust and its application to PKI and identity management, Huang and Nicol, ACM IDTrust 2009 conference proceeding, [157],

28. An anatomy of trust in public key infrastructure, Huang, Jingwei and M. Nicol, David, International Journal of Critical Infrastructures, 2017, [156],

29. The Beta Reputation System, Roslan Ismail and Audun Jøsang, 15th Bled eConference: eReality: Constructing the eEconomy, Slovenia, 2002, [164],

30. Rule-Based Trust Assessment on the Semantic Web, Jacobi I. et al. Rule-based Reasoning, Programming, and Applications - 5th International Symposium, RuleML 2011, [185],

31. Trust network analysis with subjective logic, Jøsang A., ACSC 2006 conference proceeding, [190],

32. A Policy Language for a Pervasive Computing Environment, Kagal L. et al. 4th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), Italy, [193],

33. Accountability: definition and relationship to verifiability, Küsters R. et al. Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, [211],

34. A State-Based Model for Certificate Management Systems, Chuchang Liu et al. Third International Workshop on Practice and Theory in Public Key Cryptography, PKC, Australia, 2000, [220],

35. The Eigentrust algorithm for reputation management in P2P networks, Sepandar D. Kamvar et al. Proceedings of the Twelfth International World Wide Web Conference,WWW 2003, Budapest, Hungary, 2003, [195],

36. ORDAIN: An Ontology for Trust Management in the Internet of Things, Kravari K. and Bassiliades N., On the Move to Meaningful Internet Systems. OTM 2017 Conferences - Confederated International Conferences: CoopIS, C&TC, and ODBASE 2017, [205],

37. A Language for Trust Modelling, Muller T. et al. Proceedings of the 18th International Workshop on Trust in Agent Societies co-located with the 15th International Conference on Autonomous Agents and Multiagent Systems (AAMAS, Singapore, 2016, [249],

38. PrivOnto: A semantic framework for the analysis of privacy policies, Oltramari A. et al. Semantic Web Journal 2018, [263],

39. ComTrustO: Composite trust-based ontology framework for information and decision fusion, Oltramari A. and Jin-Hee Cho, 18th International Conference on Information Fusion, FUSION 2015, Washington, DC, USA, 2015, [261],

40. CertainLogic: A Logic for Modeling Trust and Uncertainty - (Short Paper), Ries S. et al. Trust and Trustworthy Computing - 4th International Conference, TRUST Pittsburgh, PA, USA, 2011, [276],

41. Implementing Trustworthy Services Using Replicated State Machines, Fred B. Schneider and Lidong Zhou, IEEE Security & Privacy, 2005, [290],

42. Modeling and evaluation of trust with an extension in semantic web, Shekarpour and Katebi, Journal (Elsevier) Web Semantics: Science, Services and Agents on the World Wide Web, Volume 8 Issue 1, March, 2010, [302],

43. Semantic Association Identification and Knowledge Discovery for National Security Applications, Amit P. Sheth et al. J. Database Manag. 2005, [304],

44. Improving Interpretations of Trust Claims, Sel M., Trust Management X - 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Germany, [296],

45. Towards an Ontology of Trust, Viljanen L., Trust, Privacy and Security in Digital Business: Second International Conference, TrustBus 2005, Copenhagen, Denmark, [330],

46. Information accountability, Daniel J. Weitzner et al. Journal Commun. ACM, 2008, [382].

47. Model of trust management based on Finite State Machine, Caiyi Zhu and Xiangkun Dai, International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012, Kuala Lumpur, Malaysia, 2012, [391],

48. Observations on Non-repudiation, Jianying Zhou and Dieter Gollmann, Advances in Cryptology - ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Korea, 1996, [390],

49. Trust Analysis of Web Services Based on a Trust Ontology, Manling Zhu et al. Knowledge Science, Engineering and Management, Second International Conference, KSEM 2007, Melbourne, Australia, [392].

B.4 Elsevier

From Elsevier's *Journal of Web Semantics* the following articles were included.

1. Semantic Web in data mining and knowledge discovery: A comprehensive survey, Ristoski P. and Paulheim H., Journal of Web Semantics, 2016, [278],

2. Triple Pattern Fragments: A low-cost knowledge graph interface for the Web, Verborgh R. et al. Journal of Web Semantics, 2016, [327],

3. Faceted search over RDF-based knowledge graphs, Marcelo Arenas et al. Journal of Web Semantics, 2016, [8],

4. Building event-centric knowledge graphs from news, Marco Rospocher et al. Journal of Web Semantics, 2016, [279],

5. Learning the semantics of structured data sources, Mohsen Taheriyan et al. Journal of Web Semantics, 2016, [308].

From Elsevier's journal *Computers & Security* the following 5 articles were included:

1. Secure attribute-based data sharing for resource-limited users in cloud computing, Jin Li et al. Computers & Security, 2018, [217],

2. A review of cyber security risk assessment methods for SCADA systems, Cherdantseva Y. et al. Computers & Security, 2016, [56],

3. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, Kokolakis S. et al. Computers & Security, 2017, [203],

4. Information security policy compliance model in organizations, Nader Sohrabi Safa et al. Computers & Security, 2016, [284],

5. Cyber physical systems security: Analysis, challenges and solutions, Ashibani Y. et al. Computers & Security, 2017, [12].

B.5 Journal of Trust Management

A query for *semantic trust* and *semantic trustworthiness* (6/9/2019) on the website of this OpenAccess journal returned 10 articles, of which 2 were included on the basis of their relevance.

1. Efficient semi-automated assessment of annotations trustworthiness, Ceolin D. et al. Journal of Trust Management, 2014, [50],

2. Two sides of the coin: measuring and communicating the trustworthiness of online information, Nurse et al. Journal of Trust Management, 2014, [258].

B.6 DBLP

A query for articles (30/8/2019) on DBLP with *trust ontology* as search term in the period 2009 to 2019 returned 16 relevant articles.

1. Ontology-Based Reasoning about the Trustworthiness of Cyber-Physical Systems, Balduccini M. et al. CoRR Journal, 2018, [19],

2. Intercloud Trust and Security Decision Support System: an Ontology-based Approach, Bernabé J. B. et al. Journal of Grid Computing, 2015, [26],

3. A JADE-Based ART-Inspired Ontology and Protocols for Handling Trust and Reputation, Javier Ignacio Carbó Rubiera and José M. Molina López, Ninth International Conference on Intelligent Systems Design and Applications, ISDA, Italy, 2009, [280],

4. Towards an Ontology of Trust for Situational Understanding, Carpanini O. and Cerutti F., Advances in Computational Intelligence Systems - 17th UK Workshop on Computational Intelligence, 2017, UK, [44],

5. A Trust Ontology for Business Collaborations, Fatemi H. et al. Short Paper Proceedings of the 5th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling, Germany, 2012, [114],

6. UTPO: User's Trust Profile Ontology - Modeling trust towards Online Health Information Sources, Karuna P. et al, CoRR journal 2019, [198],

7. An Ontology-Based Framework Model for Trustworthy Software Evolution, Ji Li et al. Advanced Data Mining and Applications - 6th International Conference, ADMA, China, 2010, [216],

8. An Enhanced Method for Computation of Similarity between the Contexts in Trust Evaluation Using Weighted Ontology, Mohammad Amin Morid et al. IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, China, 2011, [247],

9. On the Trusted Ontology model for evaluating the Semantic Web Services, Ming Qu et al. Proceedings of the 2010 14th International Conference on Computer Supported Cooperative Work in Design, CSCWD China, 2010, [275],

10. A Trust Ontology for Semantic Services, Sherchan W. et al. 2010 IEEE International Conference on Services Computing, SCC, USA, 2010, [303],

11. Flexible Wireless Trust Through Ontology-Based Mapping and Its Attendant Semantic Limitations, Steele R. et al. Third International Conference on Network and System Security, NSS, Australia, 2009, [306],

12. Trust-terms ontology for defining security requirements and metrics, Sullivan K. et al. Software Architecture, 4th European Conference, ECSA, Denmark, 2010, [307],

13. Ontology, Epistemology, and Teleology for Modeling and Simulation - Philosophical Foundations for Intelligent M&S Applications, Tolk A., Intelligent Systems Reference Library, 2013, [312],

14. Trust Ontology Based on Access Control Parameters in Multi-organization Environments, Toumi K. et al. Ninth International Conference on Signal-Image Technology & Internet-Based Systems, SITIS 2013, Japan, [313],

15. Ontology and trust based data warehouse in new generation of business intelligence: State-of-the-art, challenges, and opportunities, Wongthongtham P. and Abu-Salih B., 13th IEEE International Conference on Industrial Informatics, INDIN, United Kingdom, 2015, [385],

16. Preference ontology-oriented metric model for trustworthy Web services, Yang Zhang et al. Int. J. Intell. Syst., 2011, [388].

B.7 Google Scholar

A query for articles (2/8/2019) published on *semantic model of trustworthiness* in the period 2014-2019 yielded *'about 17.500 results.'* The five most relevant articles selected from the first 100 articles were the following.

1. A tool for monitoring and maintaining system trustworthiness at runtime, Goldsteen et al. Workshops at 21st International Conference on Requirements Engineering: Foundation for Software Quality, Germany, 2015-03, [129], cited by 45,

2. FRTRUST: a fuzzy reputation based model for trust management in semantic P2P grids, Javanmardi et al. Computing Research Repository (CoRR), [186], cited by 91,

3. VGI edit history reveals data trustworthiness and user reputation, F D'Antonio et al. Proceedings of the AGILE'2014 International Conference on Geographic Information Science, Castellón, 2014, [159], cited by 27,

4. A decentralized trustworthy context and QoS-aware service discovery framework for the internet of things, J Li et al. IEEE Access, [215], cited by 13,

5. Towards trustworthy smart cyber-physical-social systems in the era of internet of things, J Huang et al. 11th System of Systems Engineering Conference, SoSE 2016, Norway, [158], cited by 12.

A query for articles (2/8/2019) published on *semantic model of trust* in the period 2014-2019 yielded *'about 30.600 results.'* The three most relevant articles selected from the first 100 articles were:

1. FRTRUST: a fuzzy reputation based model for trust management in semantic P2P grids, Javanmardi et al. Computing Research Repository (CoRR), [186], cited by 91,

2. A trust-based probabilistic recommendation model for social networks, Wang Y. et al. Journal of Network and Computer Applications, [381], cited by 58,

3. A trust model for data sharing in smart cities, QH Cao et al. IEEE International Conference on Communications 2016, [43], cited by 25.

As [186] already appeared in the previous search, it was selected only once.

B.8 Dedicated search for surveys and reviews

An additional search using Google Scholar and Microsoft Academic was carried out for surveys and literature reviews relevant to the research questions. This search identified 11 articles.

1. A survey of trust in computer science and the Semantic Web, Artz D. and Gil Y., Journal of Web Semantics 2007, [11],

2. A Survey on Trust Modeling, Jin-Hee Cho et al. ACM Journal Comput. Surv. 2015, [57],

3. A Review on Various Trust Models in Cloud Environment, Priya Govindaraj, Journal of Engineering Science and Technology Review 2017, [134],

4. Trust as a facilitator in cloud computing: a survey, Habib et al. J. Cloud Computing, 2012, [139],

5. Access control and the Resource Description Framework: A survey, Kirrane S. et al. Semantic Web Journal, 2016, [201],

6. Privacy, security and policies: A review of problems and solutions with semantic web technologies, Kirrane S. et al. Semantic Web Journal, 2018, [202],

7. A review on computational trust models for multi-agent systems, Lu, G. et al. ICOMP 2007 conference proceedings, [223],

8. Trust Establishment and Estimation in Cloud Services: A Systematic Literature Review, Mahmud et al. Journal of Network and Systems Management, 2019, [231],

9. Multiparty nonrepudiation: A survey, Jose Antonio Onieva et al. Journal ACM Comput. Surv., 2008, [265],

10. An Overview of PKI Trust Models, Perlman R., IEEE Network - November/December 1999, [271],

11. Trust Management Survey, Ruohomaa S. and Kutvonen L., iTrust 2005 conference proceedings, [283].

Appendix C

Shortlist

This appendix contains the shortlist of articles covered in the literature review described in Chapter 3.

C.1 Articles excluding reviews and surveys

1. A Calculus for Trust and Reputation Systems, A. Aldini, Trust Management VIII - 8th IFIP WG 11.11 International Conference, IFIPTM 2014, Singapore, July 7-10, 2014, Proceedings, [4],

2. M-STAR: A Modular, Evidence-based Software Trustworthiness Framework, N. Alexopoulos et al., CoRR, 2018, [5],

3. Ontology-Based Reasoning about the Trustworthiness of Cyber-Physical Systems, M. Balduccini et al., CoRR Journal, 2018, [19],

4. Intercloud Trust and Security Decision Support System: an Ontology-based Approach, B.J. Bernabé et al., J. Grid Comput. 2015, [26],

5. Towards an Ontology of Trust for Situational Understanding, O. Carpanini and F. Cerutti, Advances in Computational Intelligence Systems - 17th UK Workshop on Computational Intelligence, 2017, UK, [44],

6. Towards the Definition of an Ontology for Trust in (Web) Data, D. Ceolin et al., Proceedings of the 10th International Workshop on Uncertainty Reasoning for the Semantic Web (URSW 2014), [51],

7. PROVEST: Provenance-Based Trust Model for Delay Tolerant Networks, J. Cho and I. Chen, IEEE Transactions on Dependable and Secure Computing, 2018, [58]

8. A novel trust management framework for multi-cloud environments based on trust service providers, W. Fan and H. G. Perros, Journal Knowl.-Based Syst., 2014, [112],

9. Mathematical Modelling of Trust Issues in Federated Identity Management, M. S. Ferdous et al., 9th IFIP WG 11.11 International Conference, IFIPTM 2015, Hamburg, Germany, [116],

10. Computational trust methods for security quantification in the cloud ecosystem, S. M. Habib et al., The Cloud Security Ecosystem - Technical, Legal, Business and Management Issues, 2015, [140],

11. Modelling Trust Structures for Public Key Infrastructures, M. Henderson et al., Information Security and Privacy, 7th Australian Conference, ACISP 2002, Melbourne, Australia, [146]

12. An ontology of trust: formal semantics and transitivity, J. Huang and M. Fox, Proceedings of the 8th International Conference on Electronic Commerce: The new e-commerce - Innovations for Conquering Current Barriers, Obstacles and Limitations to Conducting Successful Business on the Internet, 2006, Fredericton, New Brunswick, Canada, August 13-16, 2006, [155]

13. A calculus of Trust and its application to PKI and identity management, D. Huang and J. Nicol, ACM IDTrust 2009 conference proceeding, [157],

14. An anatomy of trust in public key infrastructure, D. Huang and J. Nicol, International Journal of Critical Infrastructures, 2017, [156],

15. Rule-Based Trust Assessment on the Semantic Web, I. Jacobi et al., Rule-based Reasoning, Programming, and Applications - 5th International Symposium, RuleML 2011, [185],

16. ORDAIN: An Ontology for Trust Management in the Internet of Things, K. Kravari and N. Bassiliades, On the Move to Meaningful Internet Systems. OTM 2017 Conferences - Confederated International Conferences: CoopIS, C&TC, and ODBASE 2017, [205],

17. An Ontology Based Trust Framework for Sensor-Driven Pervasive Environment, N. Karthik and V. S. Ananthanarayana, Asia Modelling Symposium AMS, 2017, [197],

18. UTPO: User's Trust Profile Ontology - Modeling trust towards Online Health Information Sources, P. Karuna et al., CoRR journal 2019, [198],

19. A State-Based Model for Certificate Management Systems, C. Liu et al., Public Key Cryptography, Third International Workshop on Practice and Theory in Public Key Cryptography, PKC 2000, Melbourne, Victoria, Australia, [220],

20. An intelligent model for trustworthiness evaluation in semantic web applications, R. Mohammad and H. AbuMansour, 8th International Conference on Information and Communication Systems (ICICS), 2017, Jordan, [244],

21. A Language for Trust Modelling, T. Muller et al., Proceedings of the 18th International Workshop on Trust in Agent Societies co-located with the 15th International Conference on Autonomous Agents and Multiagent Systems (AAMAS, Singapore, 2016, [249],

22. ComTrustO: Composite trust-based ontology framework for information and decision fusion, A. Oltramari and J-H. Cho, 18th International Conference on Information Fusion, FUSION 2015, Washington, DC, USA, 2015, [261],

23. On the Trusted Ontology model for evaluating the Semantic Web Services, M. Qu et al., Proceedings of the 2010 14th International Conference on Computer Supported Cooperative Work in Design, CSCWD China, 2010, [275],

24. Implementing Trustworthy Services Using Replicated State Machines, F. B. Schneider and L. Zhou, IEEE Security & Privacy, 2005, [290],

25. Modeling and evaluation of trust with an extension in semantic web, S. Shekarpour and S. D. Katebi, Journal (Elsevier) Web Semantics: Science, Services and Agents on the World Wide Web, Volume 8 Issue 1, March, 2010, [302],

26. A Trust Ontology for Semantic Services, W. Sherchan et al., 2010 IEEE International Conference on Services Computing, SCC, USA, 2010, [303],

27. LogProv: Logging Events as Provenance of Big Data Analytics Pipelines with Trustworthiness, R. Wang et al., 2016 IEEE International Conference on Big Data, [380],

28. Trust Analysis of Web Services Based on a Trust Ontology, M. Zhu et al., Knowledge Science, Engineering and Management, Second International Conference, KSEM 2007, Melbourne, Australia, [392].

C.2 Reviews and surveys

1. A Survey on Trust Modeling, J-H. Cho et al., ACM Journal Comput. Surv. 2015, [57],

2. A Review on Various Trust Models in Cloud Environment, P. Govindaraj, Journal of Engineering Science and Technology Review 2017, [134],

3. Trust as a Facilitator in Cloud Computing: a Survey, S. M. Habib et al., J. Cloud Computing, 2012, [139],

4. Privacy, Security and Policies: A Review of Problems and Solutions with Semantic Web Technologies, S. Kirrane et al., Semantic Web Journal, 2018, [202],

5. Trust Establishment and Estimation in Cloud Services: A Systematic Literature Review, K. Mahmud and M. Usman, Journal of Network and Systems Management, 2019, [231],

Appendix D

Modelling and ontologies

This appendix contains a short introduction to data modelling in the OWL 2 Web Ontology Language and an overview of existing ontologies that were identified as relevant to the model described in the main body of the thesis. Where existing ontologies were used in the $\mathcal{TE}$ data model and data import functions is described.

D.1 OWL modelling in a nutshell

D.1.1 Using classes and properties

An ontology specified in the OWL 2 Web Ontology Language was created to implement the $\mathcal{TE}$ data model. The terminology defined in [148] was used. An introduction to OWL is provided in Section 4.3.6.

D.1.1.1 Classes

An ontology is a model which represents some subject matter, in the present case the $\mathcal{TE}$ model. It specifies what kind of things there are for the subject matter of interest, and how these are related to one another.

These kinds of things are called classes. The concept of class in OWL is different from e.g. the concept of a class in object oriented programming. From a semantic perspective, an OWL class corresponds to a set. OWL allows to define class hierarchy, disjointness, and class equivalence. The term 'individual' refers to the entity that is a member of a specific set. The term 'instance' is often used as a synonym.

The following class definitions are commonly used as illustration: *Person* is a class which has two subclasses, *Patient* and *Doctor*. An individual can be a member of either of these classes. The set membership can be asserted (i.e. provided as a fact), or can be inferred on the

basis of information that is already available. For example the class definition of *Patient* may impose no restrictions on class membership, it can be freely asserted that any entity which is a *Person* can be a *Patient*. However, the class of *Doctor* may define a *Doctor* as a *Person* with the imposed restriction that a *Doctor* must have the property of holding a medical degree.

Implementing a concept as a class allows the usage of a class hierarchy, disjointness, and class equivalence. It allows to create individuals as instances of the class, and to link such individuals via object properties.

D.1.1.2 Properties

Relations and predicates are expressed by properties in OWL. There are two types of properties.

- An object property relates an individual to another individual.
- A data property relates an individual to a literal.

To continue the example above, a degree could be a class, of which a specific medical degree is an individual. The restriction that a Doctor must have a medical degree can then be expressed via an object property restriction. However, when modelling under the Open World Assumption, attribute existence must be verified through queries.

D.1.2 Naming conventions

For naming classes and properties, the naming convention proposed in Uschold [323] is used, i.e. classes in upper camel case (e.g. *LegalEntity*), properties in lower camel case (e.g. *isSubsidiaryOf*).

D.1.3 Use of URIs and URI character encoding in RDF

The TE data model is implemented in OWL, using RDF/XML syntax. RDF uses URIs to represent resources. Encoding in the TE data model implementation is described as follows.

D.1.3.1 URI encoding

Encoding follows RFC 3986 [29], which specifies a URI as follows.

$$URI = scheme : [//authority]path[?query][\#fragment]$$

The RFC also defines reserved and unreserved characters for use in URIs. Reserved characters are those characters that have special meaning. For example, forward slash characters

are used to separate different parts of a URL (or more generally, a URI). Unreserved characters have no such meanings. Reserved characters need encoding.

The implementation of the TE data model uses percent-encoding, where reserved characters are represented using character sequences that start with the escape character %. For example the blank character is encoded as *%20*. Depending on the rendering, the blank might be represented as a blank ('space') character, or as *%20*. Other popular percent-encoded characters include ! (encoded as *%21*), # (encoded as *%23*), < (encoded as *%3C*) and > (encoded as *%3E*).

D.1.3.2 Carriage return encoding in XSLT

XSLT [377] is used in the data import and transformation to generate RDF. Regarding encoding, it can be observed that the XSLT way to represent a carriage return is <xsl:text>
</xsl:text>. This may introduce undesired side-effects such as carriage returns in URIs which cause rendering problems in Protégé and import problems in GraphDB. Where required such carriage returns were removed.

D.1.3.3 Encoding of special characters in XML

Regarding encoding, it can be observed that XML has a specific way to represent characters, such as *&* for & (ampersand), *<* for < (less-than), *>* for > (greater-than), *"* for " (quotation mark) and *'* for '(apostrophe). Where required these encodings were used.

D.1.4 Use of namespaces

There are some notably differences between the use of namespaces for XML and URIs. An XML namespace name does not necessarily imply any of the semantics of URI schemes. For example, a XML namespace name beginning with *http:* may have no connotation to the use of the HTTP. In XML, a namespace is an abstract domain to which a collection of element and attribute names can be assigned. The namespace name is a character string which must adhere to the generic URI syntax. However, the name is generally not considered to be a URI, because the URI specification bases the decision not only on lexical components, but also on their intended use.

The $\mathcal{TE}$ model defines its own namespace `http://www.marcsel.eu/onto/te`. The prefix *te:* is defined as a reference to the namespace. The namespaces of the imported ontologies are also used. Two further attention points were noted.

- Comments can be added directly to the ontology file with a text editor. However, when saving Protégé uses the OWL API[1] to rewrite the file, and those comments will be deleted.

[1] `https://github.com/owlcs/owlapi`

Hence comments have been stored in annotations.

- It was found more efficient to use Protégé to create the all-different general axiom than doing this manually.

D.2 Reusing existing ontologies

D.2.1 W3C ORG

D.2.1.1 Description

The W3C Organization ontology was designed by a W3C Working Group to enable publication of information on organisations and organisational structures. It is described in the W3C Organization Ontology Recommendation [376]. ORG extends and uses terms from other vocabularies, including Dublin Core [66], Friend of a Friend[37], Good Relations [228], and Provenance[357]. It defines terms to support the representation of:

- organisational structure, including notion of an organisation, decomposition into sub-organisations and units, and purpose and classification of organisations,
- reporting structure, including membership and reporting structure within an organisation, as well as roles, posts, and the relationship between people and organisations,
- location and historical information.

This coverage corresponds to the type of information typically found in organisational charts, and it does not offer a complete representation for all the nuances of organisational control structures and flows of accountability and empowerment. The ontology does not provide category structures for organisation type, purpose or roles. This ontology provides the core base concepts to allow extensions to add specific sub-class structures or classification schemes.

An illustration of the main classes and relationships in ORG is provided in Figure[2] D.1. Figure D.2 illustrates the ORG classes as loaded in Protégé.

D.2.1.2 Use in $\mathcal{TE}$ data model

The $\mathcal{TE}$ data model uses the *org:Organization* class in its specification of *te:Participant*.

[2]This figure is Copyright © [2014] World Wide Web Consortium, (MIT, ERCIM, Keio, Beihang) under licence `http://www.w3.org/Consortium/Legal/2015/doc-license`

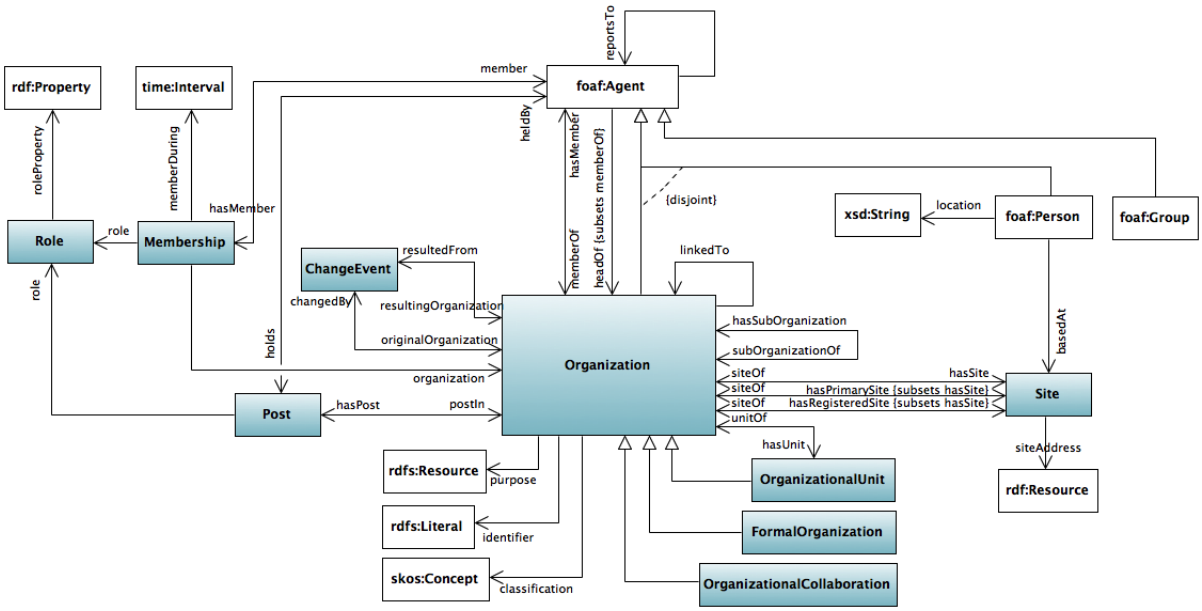

Figure D.1: W3C ORG ontology

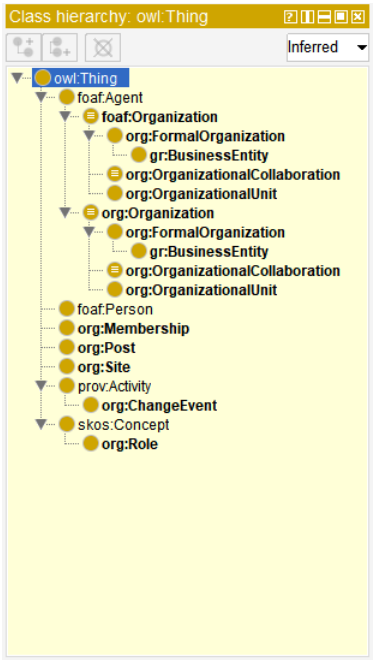

Figure D.2: W3C ORG classes loaded in Protégé

D.2.2 W3C PROV-O

D.2.2.1 Description

The Provenance ontology was defined by Moreau [245]. It consists of four recommendations:

- the PROV Data Model [355] – which describes the concepts, types and relations of the provenance data model ,
- the PROV Ontology [357], – which expresses the PROV Data model in OWL 2, also informally referred to as PROV-O,
- PROV-N [356] – a notation for provenance aimed at human consumption,
- Provenance Constraints [354] – non-mandatory validity constraints.

The three core classes of the ontology are entities, activities and agents.

- Physical, digital, conceptual, or other kinds of thing are called entities. Provenance records can describe the provenance of entities, and an entity's provenance may refer to other entities.
- Activities are how entities come into existence and how their attributes change to become new entities. They are dynamic aspects of the world, such as activities, processes, etc. For example, if the second version of a document was generated by a translation from the first version in another language, then this translation is an activity.
- An agent takes a role in an activity such that the agent can be assigned some degree of responsibility for the activity taking place. An agent can be a person, a piece of software, an inanimate object, an organization, or other entities that may be ascribed responsibility.

When an agent has some responsibility for an activity, PROV says the agent was associated with the activity. Several agents may be associated with an activity and vice-versa. An agent may be acting on behalf of others, e.g. an employee on behalf of their organization, and we can express such chains of responsibility in the provenance. It can also be described that an entity is attributed to an agent to express the agent's responsibility for that entity, possibly along with other agents. This description can be understood as a shorthand for saying that the agent was responsible for the activity which generated the entity.

The provenance of an agent can be described. For example, an organization responsible for the creation of a report may evolve over time as the report is written as some members leave and others join. To make provenance assertions about an agent in PROV, the agent must be declared explicitly both as an agent and as an entity. A role is a description of the function or the part that an entity played in an activity. Roles specify:

- the relationship between an entity and an activity, i.e. how the activity used or generated the entity,

- how agents are involved in an activity, qualifying their participation in the activity or specifying for what aspect of it each agent was responsible.

Roles are application specific, so PROV does not define any particular roles. An illustration of the main classes and relationships in PROV is provided in Figure[3] D.3. Figure D.4 illustrates the PROV classes as loaded in Protégé.

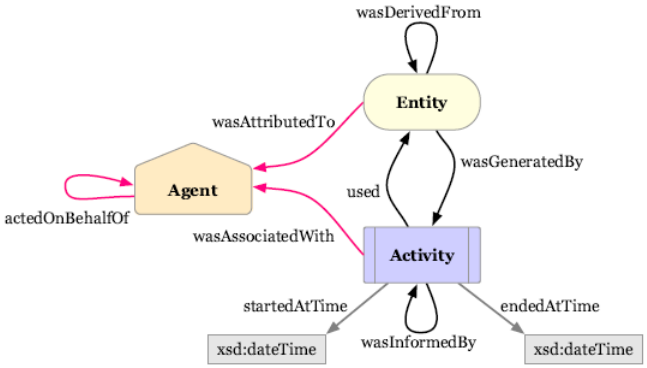

Figure D.3: W3C PROV ontology

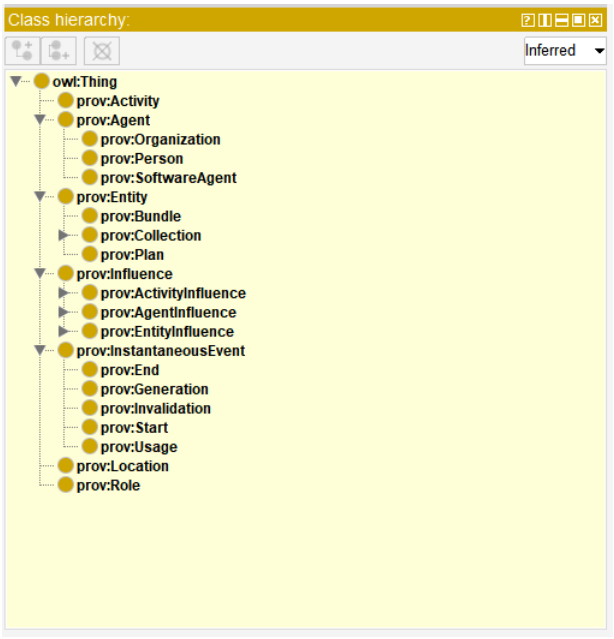

Figure D.4: W3C PROV classes loaded in Protégé

[3]This figure is Copyright © [2014] World Wide Web Consortium, (MIT, ERCIM, Keio, Beihang) under licence `http://www.w3.org/Consortium/Legal/2015/doc-license`

D.2.2.2 Use in $\mathcal{TE}$ data model

The $\mathcal{TE}$ data model uses the following provenance concepts.

- The *prov:Entity* class is used to record the source of the data used.
- The *prov:Agent* class is used to record the software agent such as the XSL program.
- The *prov:Activity* class is used to record the execution of XSL transformations and the insertion of OWL individuals in the database load file.
- The *prov:wasAttributedTo* object property records the issuer of an attestation.
  - In those cases where the issuer was a real-world entity such as a TLSO, the TLSO was referred to.
  - in those cases where the issuer was the $\mathcal{TE}$ framework software, a reference to `http://www.marcsel.eu/onto/ti/` was used[4].
- The *prov:wasGeneratedBy* object property records the activity that generated an entity such as an attestation.
- The *prov:startedAtTime* and *prov:endedAtTime*object properties record the start and end time of an activity.

D.2.3 FIBO

D.2.3.1 Introduction

The Financial Industry Business Ontology (FIBO) models business entities terms, definitions, and relationships for the purpose of the finance industry. The scope of this industry encompasses a range of organisations that manage money, including credit unions, banks, credit card companies, insurance companies, consumer finance companies, stock brokerages, investment funds and government sponsored enterprises. FIBO provides the legal and business entities concepts to support the definition of financial services entities and the relationships between them, as well as other business entities that may require financial services. The FIBO specifications consist of:

- FIBO Foundations [77],
- FIBO Business Entities [78],
- FIBO Indices and Indicators [79].

[4]The 'ti' refers to the '$\mathcal{TE}$ framework integration' software

D.2.3.2 FIBO Foundations

The FIBO Foundations specification defines a foundational set of business concepts which support the financial industry terms semantics presented in other FIBO specifications. Foundations is itself segmented into a number of ontologies and includes a number of basic legal, contractual and organizational concepts, among others. Concepts which are available in other industry standards are not included, but in some cases a 'proxy' concept is included for reference, for example for address and country concepts. The rationale for including these is the following.

- Concepts in the financial industry are generally specialisations of more general concepts such as contracts, commitments, transactions, organisations and so on. These are included in FIBO Foundations so that specialisations of them may be defined in other FIBO specifications.
- Properties of financial industry concepts frequently need to be framed in terms of relationships to non-financial concepts such as countries, jurisdictions, addresses and the like. These are included in FIBO Foundations so that properties in other FIBO specifications may make reference to them.

The FIBO model content is developed and maintained using the Unified Modeling Language as a modelling tool framework, but with all model content built using OWL constructs[5].

The FIBO Foundations ontology is published:

- as a single normative specification document [77] in pdf format[6], in human readable format,
- as a set of normative machine readable[7] specifications covering:
  - contracts,
  - arrangements,
  - documents,
  - business dates,
  - financial dates, and
  - relations.

[5]This is achieved using the OMG's Ontology Definition Metamodel (ODM) specification. This provides a means to represent OWL constructs using UML tools. This is achieved using UML's extension capability called 'profiles' for OWL and for RDF Schema. The ODM UML Profiles define a number of stereotypes which apply to standard UML metaclasses and may be used to represent OWL constructs in a consistent and meaningful way.

[6]`https://www.omg.org/spec/EDMC-FIBO/FND/1.2/PDF`

[7]Copies are available in three formats: RDF/XML serialised OWL, ODM UML XMI and ODM XMI from `https://www.omg.org/spec/EDMC-FIBO/FND/1.2/`.

D.2.3.3 FIBO Business Entities

The FIBO Business Entities specification provides general and finance domain-specific concepts that define legal and business entities, including any entity that may open an account, take out a loan, participate in any public or private offering of securities, or other business activities that require financial services (e.g., sole proprietorship, corporation, partnership, or trust, as well as governmental and not for profit organizations). The purpose is to support business scenarios such as:

- Legal Entity Identification (LEI),
- Transaction tracking, and
- Counterparty Credit Risk.

Particularly the identification of legal entities is relevant to the TE model transform/tag functionality. The scope of the concepts in FIBO Business Entities are those common to the following entities.

- Legal entities.
- Formal organizations.
- Terms definitive of or descriptive of companies incorporated by the issuance of shares and other forms of incorporated entity.
- Terms which define the existence of other kinds of legal entity.
- Terms specific to trusts.
- Terms defining the relationships for example of ownership and control between and among the kinds of organization listed above.
- Entities defined not by their legal structure but according to their role or function, including but not limited to banks, non-profit entities, government bodies, non-government and quasi-non government organizations,
- International bodies and the like.

The FIBO Business Entities ontology is published:

- as a single normative specification document [78] in PDF format[8], in human readable format,

[8] `https://www.omg.org/spec/EDMC-FIBO/BE/1.1/PDF`

- as a set of normative machine readable[9] specifications covering:
  - corporations,
  - functional entities,
  - publishers,
  - government entities,
  - EU government entities and jurisdictions,
  - UK government entities and jurisdictions,
  - CA government entities and jurisdictions,
  - US government entities and jurisdictions,
  - corporate bodies,
  - formal business organisations,
  - legal persons,
  - LEI entities,
  - control parties,
  - corporate control/ownership,
  - executives,
  - ownership parties,
  - partnerships,
  - private limited companies,
  - sole proprietorships, and
  - trusts.

D.2.3.4 Use in $\mathcal{TE}$ data import

The $\mathcal{TE}$ data import and transformation as described in Chapter 12 includes FactForge as a data source. The ontologies FIBO Foundations[10] and FIBO Business Entities [11] are loaded in FactForge. The classes *LegalEntity* and *LegalEntityIdentifier* from the ontology *fibo-be-le-lei* are used.

[9] Copies are available in two formats: RDF/XML serialised OWL and ODM XMI from `https://www.omg.org/spec/EDMC-FIBO/BE/1.1/`.

[10] version 14-11-30, November 2014

[11] version 15-02-23, February 2015

D.2.4 GLEIF

D.2.4.1 Description of the organisation

The Global Legal Entity Identifier Foundation (GLEIF) is a public domain source of identifiers and company data. The GLEIF was established by the Financial Stability Board[12] (FSB) in June 2014. It is a global not-for-profit organisation headquartered in Switzerland that supports the implementation and use of the Legal Entity Identifier (LEI). The GLEIF website[13] states that *'GLEIF makes available the Global LEI Index; i.e. a global on-line source that provides open, standardized and high quality legal entity reference data. The Global Legal Entity Identifier (LEI) Index contains historical and current LEI records including related reference data in one authoritative, central repository. The reference data provides the information on a legal entity identifiable with an LEI. The Global LEI Index is the only global on-line source that provides open, standardized and high quality legal entity reference data.'*

D.2.4.2 Oversight and use

The foundation is overseen by the LEI Regulatory Oversight Committee, representing public authorities from around the globe that drive transparency within the financial markets. The LEI Regulatory Oversight Committee publishes an overview[14] of where the use of the LEI has been made mandatory or strongly suggested. This includes most territories worldwide.

D.2.4.3 GLEIF ontologies

GLEIF publishes 4 ontologies:

- The GLEIF level 1 ontology [123] , referred to as *Who is Who*, covers key reference data for a legal entity identifiable with an LEI. It builds on ISO 17442 [165].
  - A legal entity is defined in the GLEIF level 1 ontology as *'LEI-registered entities that are legally or financially responsible for the performance of financial transactions or have the legal right in their jurisdiction to enter independently into legal contracts, regardless of whether they are incorporated or constituted in some other*

[12]The Financial Stability Board (FSB) is an international body that monitors and makes recommendations about the global financial system. It was established after the G20 London summit in April 2009 and includes all G20 major economies, Financial Stability Forum (FSF) members, and the European Commission. Hosted and funded by the Bank for International Settlements, the board is based in Basel, Switzerland. The FSB has 68 member institutions, comprising ministries of finance, central banks, and supervisory and regulatory authorities from 25 jurisdictions as well as 10 international organizations and standard-setting bodies, and 6 Regional Consultative Groups reaching out to 65 other jurisdictions around the world.

[13]`https://www.gleif.org/en/`, last accessed on 19 January 2021

[14]`https://www.leiroc.org/lei/uses.htm` last accessed on 19 January 2021

way (e.g. trust, partnership, contractual). It excludes natural persons, but includes governmental organizations and supranationals.'

- A Legal Entity Identifier (LEI) is defined in the GLEIF level 1 ontology as *'The ISO 17442 compatible identifier for the legal entity referenced.'* It consists of 20 characters:
  - Characters 1-4: Prefix used to ensure the uniqueness among codes from LEI issuers (Local Operating Units or LOUs).
  - Characters 5-18: Entity-specific part of the code generated and assigned by LOUs according to transparent, sound and robust allocation policies. As required by ISO 17442, it contains no embedded intelligence.
  - Characters 19-20: Two check digits as described in the ISO 17442 standard.

  The ISO 17442 standard specifies the minimum reference data which are the following.
  - The official name of the legal entity as recorded in the official registers.
  - The registered address of that legal entity.
  - The country of formation.
  - The codes for the representation of names of countries and their subdivisions.
  - The date of the first LEI assignment; the date of last update of the LEI information; and the date of expiry, if applicable.
- A local operating unit is defined in the GLEIF level 1 ontology as *"An entity that supplies registration, renewal and other services, and acts as the primary interface for legal entities wishing to obtain an LEI. Only organizations duly accredited by the Global Legal Entity Identifier Foundation (GLEIF) are authorized to issue LEIs."*

- The GLEIF level 2 ontology [124] , referred to as *Who Owns Whom*, allows to describe legal entity parent relationships.

- The Entity Legal Form (ELF) ontology [122] defines concepts for Entity Legal Forms and their abbreviations by jurisdiction, based on ISO 20275 [166]. The current version of the ELF ontology, released in July 2019, lists more than 2,100 entity legal forms across more than 90 jurisdictions. The list contains legal forms/types in their native language, such as limited liability companies (Ltd), Gesellschaft mit beschränkter Haftung (GmbH) or Société Anonyme (SA).

- Registration Authority ontology [125] defining concepts for Business Registries, including the jurisdictions served.

D.2.4.4 GLEIF data

Access to GLEIF data is available through at least the following methods.

- A web-based search tool and a file download service is offered by GLEIF to access the publicly available LEI data pool. The data is only available in such large datasets that these cannot be opened, queried or processed by regular applications, editors or browsers. It is intended to be processed by dedicated applications that process the data in streaming mode.
- DTCC, an American company, offers a *Global Markets Entity Identifier* Utility to access its data in collaboration with SWIFT.
- The data is integrated in Linked Open Data sources such as FactForge which can be queried on-line and from where data can be downloaded.

D.2.5 Linked Open Data

The term *Linked Open Data* refers to data that is both *Linked Data* and *Open Data*. *Linked Data* is a term commonly used to refer to data that complies to Tim Berners-Lee's four principles[15] formulated in 2006:

1. Use URIs as names for things,
2. Use HTTP URIs so that people can look up those names,
3. When someone looks up a URI, provide useful information, using the standards (RDF*, SPARQL),
4. Include links to other URIs so that they can discover more things.

Open Data is a term commonly used to refer to data that can be freely used and distributed by anyone, subject only to the requirement to attribute and share-alike. *Linked Open Data* refers to data that complies with both terms. It is both linked and uses open sources. There are many sources of Linked Open Data. The W3C offers an overview of well-known data sets available in RDF at `https://www.w3.org/wiki/DataSetRDFDumps`.

D.2.6 DBpedia

DBpedia is a well-studied example of Linked Open Data.

[15] `https://www.w3.org/DesignIssues/LinkedData.html`

- It extracts structured information from Wikipedia and makes it available through its public SPARQL endpoint[16].
- It is developed by the Leipzig University, the University of Mannheim, and OpenLink Software.
- There is large body of academic publications available regarding DBpedia[17].

D.2.6.1 Data extraction

DBpedia extracts data from Wikipedia's infoboxes. An infobox is a table used to collect and present a subset of information about its subject. It is a structured document containing a set of attribute–value pairs, and represents a summary of information about the subject of a Wikipedia article. Each attribute-value pair of an infobox is extracted into an RDF triple according to the DBpedia ontology. Each type of infobox is mapped to an ontology class, and each property within an infobox is mapped to an ontology property.

For example the English Wikipedia article about London contains a 'settlement' infobox. This infobox may be mapped to e.g. the class 'populated place' in the DBpedia ontology and the attributes in the infobox are mapped to properties in the DBpedia ontology. This allows to obtain a unified view over all data in infoboxes. Since this information conforms to Semantic Web standards, it can be queried and combined by a broad range of tools.

D.2.6.2 DBpedia ontology

The DBpedia ontology is based on OWL and describes classes, e.g. person, city, country, and properties, e.g. birth place, longitude. Information in Wikipedia articles is then mapped via the above described mapping to this ontology.

For naming things, on top of well-known ontologies such as Dublic Core, FOAF, OWL, SKOS etc. DBpedia uses its own ontology. According to its website[18] the ontology[19] covers 685 classes which form a subsumption hierarchy and are described by 2,795 different properties.

DBpedia defined the following namespaces:

- dbo *http://dbpedia.org/ontology/*
- dbp *http://dbpedia.org/property/*
- dbr *http://dbpedia.org/resource/*

[16] `https://dbpedia.org/sparql`
[17] `https://dblp.uni-trier.de/search?q=DBpedia`
[18] `https://wiki.dbpedia.org/services-resources/ontology`, last visited 21 January 2021
[19] `http://mappings.dbpedia.org/server/ontology/classes`, last visited 21 January 2021

- dbr-de *http://de.dbpedia.org/resource/*

The full list of namespaces can be obtained on-line[20].

D.2.7 Wikidata

Wikidata is another example of Linked Open Data. Wikidata acts as central storage for the structured data of its Wikimedia sister projects including Wikipedia, Wikivoyage, Wiktionary, Wikisource, and others. The data on Wikidata is added by a community of volunteers both manually and by using software, like other Wikimedia projects including Wikipedia.

For naming things, Wikidata has its own way of identifying things and allocating properties to them. The Wikidata repository consists mainly of items, each one having a label, a description and any number of aliases. Items are uniquely identified by a character Q followed by a number, such Q42. Statements describe characteristics of an Item and consist of a property and a value. Properties in Wikidata have a character P followed by a number, such as with educated at(P69). Properties can also link to external databases. A property that links an item to an external database, such as an authority control database used by libraries and archives, is called an identifier. Wikidata offers a public SPARQL query service. There is also a large body of academic publications available regarding Wikidata[21].

D.2.8 Other examples

Other examples include FactForge, described in Appendix I.4, as well as output from projects by the Open Knowledge Foundation[22], and LinkedData.org[23].

[20] `https://dbpedia.org/sparql?nsdecl`, last accessed 21 January 2021
[21] `https://dblp.uni-trier.de/search?q=wikidata`
[22] `https://okfn.org/`
[23] `https://linkeddata.org/`

Appendix E

$\mathcal{TE}$ data model specification in DL

The $\mathcal{TE}$ model that is specified in Chapter 11 is provided here in Description Logic syntax.

The DL specification of the model is provided below, using the syntax defined by Baader et al. [325].

Classes

Accreditation

Accreditation $\sqsubseteq$ Attestation

Agreement

Agreement $\sqsubseteq$ TemporalRelation

Attestation

Attestation $\sqsubseteq$ TemporalRelation

Conformance

Conformance $\sqsubseteq$ Attestation

Disclosure

Disclosure $\sqsubseteq$ Attestation

Endorsement

Endorsement $\sqsubseteq$ TemporalRelation

Enforcement

Enforcement $\sqsubseteq$ TemporalRelation

Event

Event $\sqsubseteq$ TimeInterval

ID

ID $\equiv \exists$ uniqueText Datatype http://www.w3.org/2001/XMLSchema#string
ID $\sqsubseteq \neg$ LivingThing

IdentityAttestation

IdentityAttestation $\sqsubseteq$ Attestation

Interaction

Interaction $\sqsubseteq$ Event

LegalNorm

LegalNorm $\sqsubseteq$ Norm

LegalPerson

LegalPerson $\equiv$ Organization $\sqcap \exists$ name Datatype http://www.w3.org/2001/XMLSchema#string

LegalQualification

LegalQualification $\sqsubseteq$ Attestation

LivingThing

LivingThing $\sqsubseteq \neg$ RuleBook
LivingThing $\sqsubseteq \neg$ TimeInterval
LivingThing $\sqsubseteq \neg$ ID
LivingThing $\sqsubseteq \neg$ TimeInstant

NaturalPerson

NaturalPerson ≡ LivingThing ⊓ ∃ name Datatype http://www.w3.org/2001/XMLSchema#string

Norm

Organization

Participant

Participant ≡ Thing ⊓ NaturalPerson ⊔ Organization ⊓ ∃ identifiedBy ID
Participant ⊑ ¬ TimeInterval
Participant ⊑ ¬ RuleBook
Participant ⊑ ¬ TimeInstant

Registration

Registration ⊑ Attestation

Role

Role ≡ {AB} ⊔ {AS} ⊔ {CAB} ⊔ {CsSP} ⊔ {EnDo} ⊔ {EnFo} ⊔ {EvSP} ⊔ {FuSC} ⊔ {FuSP} ⊔ {TwsMo}

RoleAttestation

RoleAttestation ⊑ Attestation

RuleBook

RuleBook ⊑ ¬ LivingThing
RuleBook ⊑ ¬ TimeInterval
RuleBook ⊑ ¬ TimeInstant
RuleBook ⊑ ¬ Participant

Standard

Standard ⊑ Norm

Supervision

Supervision ⊑ Attestation

TemporalRelation

TemporalRelation ⊑ TimeInterval

Thing

TimeInstant

TimeInstant ⊑ ¬ RuleBook
TimeInstant ⊑ ¬ LivingThing
TimeInstant ⊑ ¬ Participant

TimeInterval

TimeInterval ⊑ ¬ Participant
TimeInterval ⊑ ¬ RuleBook
TimeInterval ⊑ ¬ LivingThing

Object properties

aConformance

∃ aConformance Thing ⊑ Attestation
⊤ ⊑ ∀ aConformance Conformance

accreditationN

∃ accreditationN Thing ⊑ Accreditation
⊤ ⊑ ∀ accreditationN Norm

agreementR

∃ agreementR Thing ⊑ Agreement
⊤ ⊑ ∀ agreementR RuleBook

conformanceN

∃ conformanceN Thing ⊑ Conformance
⊤ ⊑ ∀ conformanceN Norm

doesIdentify

doesIdentify $\equiv$ identifiedBy^{-}
$\top \sqsubseteq \leq 1$ doesIdentify Thing
$\exists$ doesIdentify Thing $\sqsubseteq$ ID
$\top \sqsubseteq \forall$ doesIdentify Thing

endorsementR

$\exists$ endorsementR Thing $\sqsubseteq$ Endorsement
$\top \sqsubseteq \forall$ endorsementR RuleBook

endsOn

$\top \sqsubseteq \forall$ endsOn TimeInstant

enforcementR

$\exists$ enforcementR Thing $\sqsubseteq$ Enforcement
$\top \sqsubseteq \forall$ enforcementR RuleBook

identifiedBy

doesIdentify $\equiv$ identifiedBy^{-}
$\exists$ identifiedBy Thing $\sqsubseteq$ Thing
$\top \sqsubseteq \forall$ identifiedBy ID

identityAttestationID

$\sqsubseteq$ topObjectProperty
$\exists$ identityAttestationID Thing $\sqsubseteq$ IdentityAttestation
$\top \sqsubseteq \forall$ identityAttestationID ID

interactionHasEvidence

$\exists$ interactionHasEvidence Thing $\sqsubseteq$ Interaction

legalQualificationN

$\exists$ legalQualificationN Thing $\sqsubseteq$ LegalQualification
$\top \sqsubseteq \forall$ legalQualificationN Norm

pAccreditation

$\exists$ pAccreditation Thing $\sqsubseteq$ Participant
$\top \sqsubseteq \forall$ pAccreditation Accreditation

pAgreement

$\exists$ pAgreement Thing $\sqsubseteq$ Participant
$\top \sqsubseteq \forall$ pAgreement Agreement

pConformance

$\exists$ pConformance Thing $\sqsubseteq$ Participant
$\top \sqsubseteq \forall$ pConformance Conformance

pDisclosure

$\exists$ pDisclosure Thing $\sqsubseteq$ Participant
$\top \sqsubseteq \forall$ pDisclosure Disclosure

pEndorsedBy

pEndorsedBy $\equiv$ pEndorsement$^-$

pEndorsement

pEndorsedBy $\equiv$ pEndorsement$^-$
$\exists$ pEndorsement Thing $\sqsubseteq$ Participant
$\top \sqsubseteq \forall$ pEndorsement Endorsement

pEnforcedBy

pEnforcedBy $\equiv$ pEnforcement$^-$

pEnforcement

pEnforcedBy $\equiv$ pEnforcement$^-$
$\exists$ pEnforcement Thing $\sqsubseteq$ Participant
$\top \sqsubseteq \forall$ pEnforcement Enforcement

pIdentityAttestation

$\exists$ pIdentityAttestation Thing $\sqsubseteq$ Participant
$\top \sqsubseteq \forall$ pIdentityAttestation IdentityAttestation

pLegalQualification

$\exists$ pLegalQualification Thing $\sqsubseteq$ Participant
$\top \sqsubseteq \forall$ pLegalQualification LegalQualification

pRoleAttestation

$\exists$ pRoleAttestation Thing $\sqsubseteq$ Participant
$\top \sqsubseteq \forall$ pRoleAttestation RoleAttestation

pSupervision

$\exists$ pSupervision Thing $\sqsubseteq$ Participant
$\top \sqsubseteq \forall$ pSupervision Supervision

participatesInInteraction

$\exists$ participatesInInteraction Thing $\sqsubseteq$ Participant

raLegalQualification

$\exists$ raLegalQualification Thing $\sqsubseteq$ RoleAttestation
$\top \sqsubseteq \forall$ raLegalQualification LegalQualification

roleAttestationR

$\exists$ roleAttestationR Thing $\sqsubseteq$ RoleAttestation
$\top \sqsubseteq \forall$ roleAttestationR Role

startsOn

$\top \sqsubseteq \forall$ startsOn TimeInstant

supervisionP

$\exists$ supervisionP Thing $\sqsubseteq$ Supervision
$\top \sqsubseteq \forall$ supervisionP Participant

topObjectProperty

underRuleBook

$\top \sqsubseteq \forall$ underRuleBook RuleBook

Data properties

DisclosureURI

$\exists$ DisclosureURI Datatypehttp://www.w3.org/2000/01/rdf-schema#Literal $\sqsubseteq$ Disclosure
$\top \sqsubseteq \forall$ DisclosureURI Datatypehttp://www.w3.org/2001/XMLschema#anyURI

NormURI

$\exists$ NormURI Datatypehttp://www.w3.org/2000/01/rdf-schema#Literal $\sqsubseteq$ Norm
$\top \sqsubseteq \forall$ NormURI Datatypehttp://www.w3.org/2001/XMLschema#anyURI

RegisterURI

$\exists$ RegisterURI Datatypehttp://www.w3.org/2000/01/rdf-schema#Literal $\sqsubseteq$ Registration
$\top \sqsubseteq \forall$ RegisterURI Datatypehttp://www.w3.org/2001/XMLSchema#anyURI

RuleSet

$\top \sqsubseteq \forall$ RuleSet Datatypehttp://www.w3.org/2001/XMLSchema#string

name

ruleBook-digest-RIPEMD-160

$\top \sqsubseteq \leq 1$ ruleBook-digest-RIPEMD-160
$\top \sqsubseteq \forall$ ruleBook-digest-RIPEMD-160 Datatypehttp://www.w3.org/2001/XMLSchema#string

ruleBook-digest-SHA-256

$\top \sqsubseteq \leq 1$ ruleBook-digest-SHA-256
$\top \sqsubseteq \forall$ ruleBook-digest-SHA-256 Datatypehttp://www.w3.org/2001/XMLSchema#string

uniqueText

$\top \sqsubseteq \leq 1$ uniqueText
$\top \sqsubseteq \forall$ uniqueText Datatypehttp://www.w3.org/2001/XMLSchema#string

Individuals

AB

AS

CAB

CsSP

EnDo

EnFo

EvSP

FuSC

FuSP

TwsMo

Datatypes

PlainLiteral

anyURI

string

Appendix F

Trusted lists

This appendix provides background information on the European trusted lists that were implemented as a consequence of the eIDAS regulation [103].

F.1 Introduction

The European trusted lists were established as part of the implementation of the eIDAS Regulation [103], which was described in Section 2.2.3.1. It included the organisation of a European scheme of trusted lists[1] published by national Trusted List Scheme Operators (TLSOs).

F.2 Purpose of trusted lists

The purpose of a trusted list is to allow a TLSO to provide information about the status and status history of the trust services from Trust Service Providers (TSPs) regarding compliance with the relevant provisions of the applicable legislation on digital signatures and trust services for electronic transactions. This information is provided for the benefit of parties that want to rely on the trust services provided by those TSPs.

It can be observed that some of these TSPs (e.g. Certipost, the TSP for the Belgian electronic identity card) do not limit themselves to eSignature services, but also provide identity-related services.

The specification ETSI TS 119 612 [89] states the following.

EU Member States' trusted lists were established in EU by Commission Decision 2009/767/EC and aimed primarily at supporting the validation of advanced electronic signatures supported by a qualified certificate and advanced electronic signature supported by both a qualified certificate and by a secure signature creation device, in the meaning of Directive 1999/93/EC,

[1] The terms trusted list and trust list are frequently used interchangeable, and are considered as such here also. The defining specification, ETSI TS 119 612 [89] uses the term 'Trusted Lists' so this is used in the thesis as well.

as far as they included as a minimum trust service providers supervised/accredited for issuing qualified certificates. TLSOs could however include in their trusted lists also other types of approved trust service providers. Hence, the cross-border use of electronic services based on advanced electronic signatures is also facilitated, where the supporting trust services (e.g. issuing of non-qualified certificates) are part of the listed supervised/accredited services.

Regulation (EU) No 910/2014 [i.10] extends the scope of qualified trust services and trust service providers to a wider but definite list of harmonised trust services. The Regulation is applicable as of 1 July 2016, until when the Commission Decision 2009/767/EC [i.2], as amended, remains applicable. For trust services not covered by the Regulation, Member States remain free to define other types of trust services, for national purposes where these can be considered as qualified trust services (without effect in other Member States).

An assessment scheme for Conformity Assessment Bodies to assess TSPs is specified in ETSI EN 319 403 [88].

An overview of the Trust Service Providers listed in the TLs is publicly available[2] in a dashboard. A screenshot of the dashboard, captured on 2 April 2021, is shown in Figure F.1.

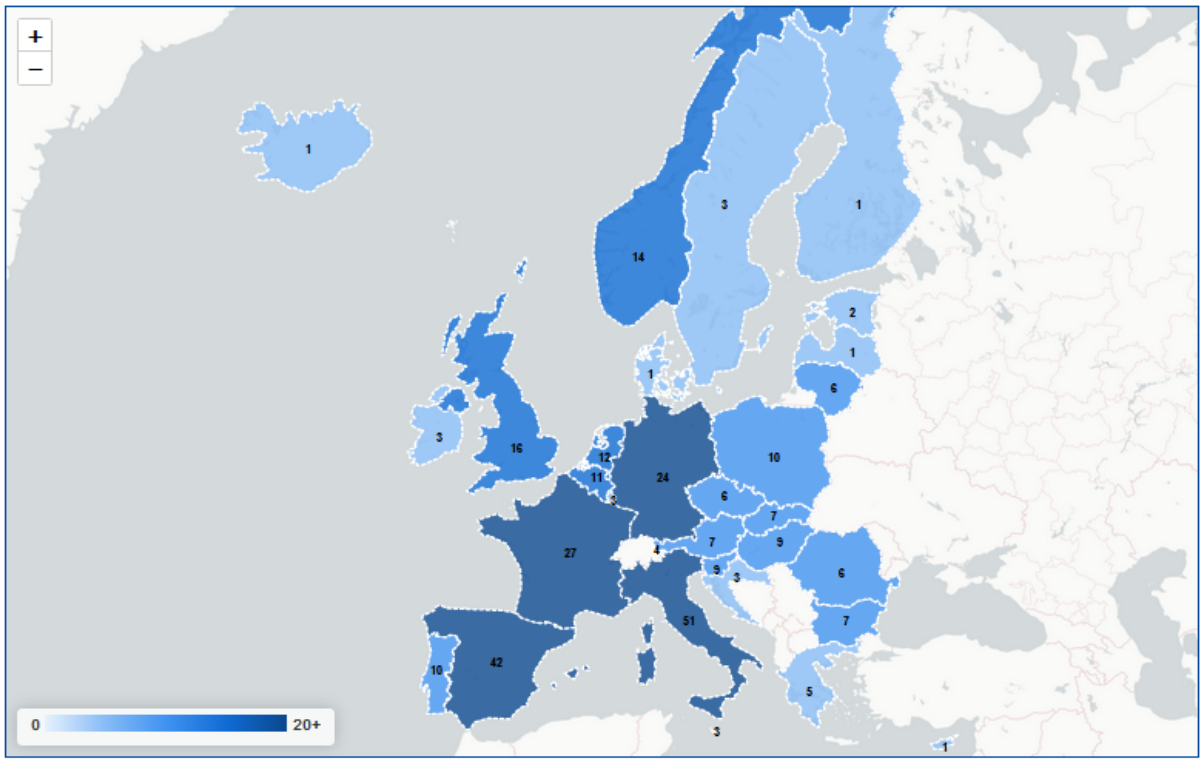

Figure F.1: eIDAS TL dashboard

Each trusted list provides information about the status and history of the trust services of

[2] https://webgate.ec.europa.eu/tl-browser/\#/dashboard

the included Trust Service Providers (TSPs) regarding compliance with the relevant legislation. Two observations are in order.

- While the eIDAS Regulation [103] does not classify identity and authentication services as trust services, some TSPs (e.g. the TSP for the Belgian electronic identity card) do not limit themselves to eSignature services, but also provide identity-related services[3].
- The eIDAS classification of trust services is specified in eIDAS [103] Art. 3. It includes the creation and the verification of a signature, which may be executed locally or remotely. Using the $\mathcal{TE}$ data model terminology, such a verification is performed by a claim status service provider. It can be observed that in practice there are only a few companies that offer verification services. Therefore claim status service providers are out of scope for the implementation. More background information is provided in appendix F.7.

F.3 Availability

The TLs are made available at country-specific locations (URIs). Both a human readable (PDF) and machine readable (XML) version are published. For example the Belgian machine readable TL can be found at `http://tsl.belgium.be/tsl-be.xml`. Replacing the suffix *.xml* by *.pdf* returns the human readable version.

The trusted lists are also available through the graphical user interface of the trusted list browser[4]. The location and the identity of the TL issuers can be checked in the European List of Trusted Lists, available at `https://ec.europa.eu/tools/lotl/eu-lotl.xml`.

F.4 Formalisation

F.4.1 Standardisation and terminology

Trusted lists are created according to ETSI TS 119 612 [89]. The specification allows to allocate the responsibilities for supervision, accreditation and scheme operation to a single actor, or to separate them. According to ETSI TS 119 612 [89] Section 5.3.7, the allocation of responsibilities should be indicated. This allocation is different per Member State.

ETSI TS 119 612 [89] Section 3 contains definitions in natural language. These are based on legislation. Section 4 explains the overall structure of Trusted Lists. Section 5 defines format and content. These are specified in terms of presence (required or not), description (in natural language), format, and value (explaining the different possible values).

[3] This includes certificates for authentication and signature keys.

[4] `https://webgate.ec.europa.eu/tl-browser/` or `https://esignature.ec.europa.eu/efda/tl-browser/\#/screen/home`

Annex B specifies the XML implementation, and includes references to three XML schema definition files (.xsd). The latter specify the actual types.

ETSI standarisation work also includes the use of Object Identifiers (OIDs) to standardise the meaning of information fields. ETSI leverages the ITU-T Object Identifiers, and as a consequence, today's certificates may contain various OIDs, such as the Qualified Certificate (QC) Profile OID (0.4.0.1862) which refers to ETSI TS 101 862 (QCP). The presence of this OID within the certificate indicates it is qualified as per the ETSI Technical Specification.

ETSI TS 119 612 [89] includes the following terms and definitions in section 3.1:

- approval: assertion that a trust service, falling within the oversight of a particular scheme, has been either positively endorsed or assessed for compliance against the relevant requirements (active approval) or has received no explicit restriction since the time at which the scheme was aware of the existence of the said service (passive approval)
- approval scheme: any organized process of supervision, monitoring, assessment or such practices that are intended to apply oversight with the objective of ensuring adherence to specific criteria in order to maintain trust in the services under the scope of the scheme
- conformity assessment: process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled
- scheme operator: body responsible for the operation and/or management of any kind of assessment scheme, whether they are governmental, industry or private, etc.
- supervision system: system that allows for the supervision of trust service providers and the services they provide, for compliance with relevant requirements
- trust service: electronic service which enhances trust and confidence in electronic transactions
- Trust Service Provider (TSP): body operating one or more (electronic) trust services
- Trust Service Token (TrST): physical or binary (logical) object generated or issued as a result of the use of a trust service NOTE: Examples of binary trust service tokens are: certificates, CRLs, time-stamp tokens, OCSP responses. Physical tokens can be devices on which binary objects (tokens or credentials) are stored. Equally, a token can be the performance of an act and the generation of an electronic record, e.g. an insurance policy or share certificate.
- Trusted List (TL): list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation. NOTE: In the

context of European Union Member States, as specified in Regulation (EU) No 910/2014 [i.10], it refers to a EU Member State list including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them. In the context of non-EU countries or international organizations, it refers to a list meeting the requirements of the present document and providing assessment scheme based approval status information about trust services from trust service providers, for compliance with the relevant provisions of the applicable approval scheme and the relevant legislation.

- (voluntary) accreditation: any permission, setting out rights and obligations specific to the provision of trust services, to be granted upon request by the trust service provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the trust service provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body

F.4.2 Formalisation in XML

TLs are specified in XML version 1 using UTF-8 encoding. The top-level element of a TL is a *tsl:TrustServiceStatusList*, which contains a *tsl:SchemeInformation* element as first sub-element. The latter contains a *tsl:TSLType* tag that identifies the trusted list type (e.g. 'generic' as shown).

```
1 <tsl:TSLType>
2 http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/
    TSLType/generic
3 </tsl:TSLType>
```

F.4.2.1 TLSO

Within the *tsl:SchemeInformation* element, the Member State Competent Authority is specified as Scheme Operator using the <*tsl:SchemeOperatorName*> tag.

F.4.2.2 Endorsement

Also within the *tsl:SchemeInformation* element, a pointer to the European Commission's List of Trusted Lists is provided.

```
1 <TSLLocation>https://ec.europa.eu/tools/lotl/eu-lotl.xml</
    TSLLocation>
```

Under <*AdditionalInformation*> the European Commission is specified by the <*Scheme-OperatorName*> as operator of the LOTL scheme. This represents an endorsement from the Member State to the European Commission's trusted list[5]

F.4.2.3 TSPs

The TSPs included in the scheme are specified in a list which is identified by the tag <*tsl:TrustServiceProviderList*>. Within this list, individual TSPs are specified in <*tsl:TrustServiceProvider*> elements, which contain a <*tsl:TSPInformation*> element.

The latter contain elements such as <*tsl:TSPName*> (e.g. Certipost NV/SA), and an element <*tsl:TSPServices*> which contains the individual descriptions of <*tsl:TSPService*> and its <*tsl:ServiceInformation*>.

The latter contains a <*tsl:ServiceTypeIdentifier*> (e.g. http://uri.etsi.org/TrstSvc/Svctype/CA/QC), a <*tsl:ServiceName*>, a <tsl:ServiceStatus> (e.g. http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision)

Further details are provided under the <*tsl:ServiceInformationExtensions*> element.

F.4.2.4 Signature

The last element, <*ds:Signature*>, contains a digital signature of the TLSO over the XML structure.

F.5 Comparison of transformation alternatives

F.5.1 XSL Transformations (XSLT) and XPath

Extensible Stylesheet Language Transformations (XSLT) [377] is a language for transforming XML documents into other XML documents. It is commonly used with Xpath [334] which is a language for identifying particular parts of XML documents.

XSLT is the first part of the XSL stylesheet language for XML. It is a Turing-complete language that includes the XSL Transformation vocabulary and XPath, a language for addressing parts of XML documents. The XSLT language allows to write XSL stylesheets which contain instructions for transforming one tree of nodes (the XML input) into another tree of nodes (the output or transformation result). As Trusted Lists are available in XML they can be used as input. XSLT allows to add/remove elements and attributes to or from the output file. It also allows to rearrange and sort elements, perform tests and make decisions about which elements to hide and display. In this transformation process, XSLT uses XPath to define parts of the

[5]The LOTL itself contains a reference to the trusted lists of the Member States. This represents an endorsement from the European Commission to the Member State trusted list.

source document that should match one or more predefined templates. When a match is found, XSLT will transform the matching part of the source document into the result document.

XPath is a language for identifying particular parts of XML documents. It allows to write expressions to select elements and attributes of the input on the basis of position, relative position, type, content and other criteria. From the perspective of XPath, an XML document is a tree made up of nodes, which may be nested. XPath distinguishes seven types of nodes: root, element, text, attribute, comment, processing instruction and namespace nodes.

F.5.2 Jena

Jena is a collection of Open Source software modules which implements APIs for OWL, RDF, SPARQL, reasoners, storage, parsing and writing (XML, N3, turtle, ...). Jena also offers its own triples stores, Fuseki and TDB. Jena stores everything in RDF. The RDF document(s) contain 'statements' (i.e. triples). The Jena APIs support the following interfaces:

- Model: a set of statements (ontology model, inference model),
- Statement: a triple of {R, P, O},
- Resource: subject, URI,
- Property: 'item' of resource,
- Object: may be a resource or a literal,
- Literal: non-nested 'object',
- Container: special resource, collection of things.

F.5.3 SPIN

The SPARQL Inferencing Notation (SPIN) allows to represent SPARQL rules and constraints on Semantic Web models. SPIN also provides meta-modelling capabilities that allow users to define their own SPARQL functions and query templates. SPIN also includes a library of common functions. More information can be found at its website[6]. SPIN is supported in various tools, including in the GraphDB Workbench's OntoRefine function. The origin of SPIN is a W3C Member Submission[7]. Its concepts have given rise to W3C's SHACL[8]. From a transformation perspective, SPIN functions support parsing, splitting and encoding which can be used in a SPARQL construct statement to create triples.

[6] `https://spinrdf.org/`
[7] `https://www.w3.org/Submission/2011/SUBM-spin-overview-20110222/`
[8] `https://www.w3.org/TR/shacl/`

F.5.4 Conclusion

Comparison:

- The capabilities of XLST and XPath match well with the task at hand, because these languages have been created for the very purpose.
- The capabilities of Jena match less. Jena offers an API to work with triples however it is less oriented towards the creation of such triples. Working with triples is less relevant since the main work consists of creation and later executing the TWSEVAL, which are implemented in SPARQL.
- The capabilities of SPIN match less. While it seems possible to use SPIN (or SHACL) for the required transformations, a comparison of how this would have to be programmed on the basis of the available documentation indicates it is more labour intensive than the XSLT and XPath approach.

As a consequence, XSLT and XPath are selected to specify the transformations.

F.6 Implementation of the transformations

F.6.1 Approach

Xalan-Java was used to specify and execute the transformations. It is an Open Source implementation[9] of W3C XSL Transformations (XSLT) Version 1.0 [377] and the XML Path Language (XPath) Version 1.0 [334] recommendations.

Trusted lists are published in XML format which is transformed into RDF triples by XSLT. This is done by specifying a series of XSL transformations and subsequently executing these through a Java program over the XML input. The execution results in RDF output.

- Creation of an XSL transformer instance using the specified XSL transformation.
- Loading of the XML into memory.
- Execution of the XSL transformer over the XML.

Fig F.2 shows the flow of execution.

[9] `http://xml.apache.org/`

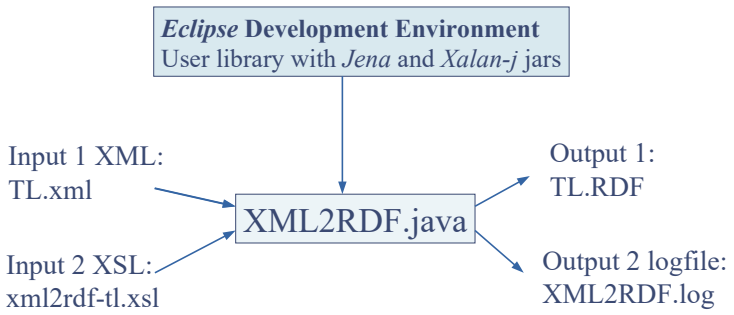

Figure F.2: XSL transformation from XML to RDF.

F.6.2 Input

The input consists of an XML document, which contains elements, structured by tags. Elements may have attributes. Consider a sample document structured as

<person born=”1912-06-23”> Alan Turing </person>

This document has one element, created by the *person* tag. Which has one attribute (*born*). Tags can be nested.

F.6.3 Transformation

The following is required.

- According to the W3C XSLT Recommendation [377] an XSL style sheet needs to start with:

  <xsl:transform version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">

- To get access to the XSLT elements, attributes and features the XSLT namespace must be declared at the top of the document.

XSLT allows to select elements from the input tree using an Xpath expression and using them to create elements and attributes in the output tree. The instruction

<xsl:template match="matcher">

iterates over the input tree and tries to match against what is specified as "matcher".

For example

<xsl:template match="tsl:TrustServiceStatusList">

matches against the toplevel element of a TL. The 'matcher' is an XPath expression which can be can be absolute or relative.

- Absolute means the path starts from the root of the input tree, '/'.
- Relative means the path starts from the context node, i.e. the node currently selected. The context node itself is selected with a dot '.'. Its parent is selected with a double dot '..', and its descendants with a double slash '//'.

The instructions *xsl:element* and *xsl:attribute* insert an element and an attribute respectively. Assigning the value that is inserted can be done a.o. via *xsl:value-of* which selects the string value of an XPath expression, or via the an interim *xsl:variable*, which also selects the string value of an XPath expression and can then be used in an expression referenced by its $name.

F.7 Claim status service providers

F.7.1 Selection of alternatives

The role of claim status service provider is specified in 6.5.2. In today's landscape of electronic service providers, it can be observed that most evidence service providers (such as TSPs, CAs, IdPs) mostly provide certificates such as X.509 certificates. Some provide evidence creation services such as signature creation. However, the number of service providers that e.g. verify a signature are limited. It is assumed that a relying party has its own verification software at its disposal. Adobe Acrobat, Windows Office, LibreOffice and other software offer this possibility. As this expects users to know how to configure and perform the verification operations, on-line verification services are increasingly available.

F.7.2 Implementation

Two claim status service providers are briefly discussed as examples. The first service provider is offered by the Belgian Federal Government. The Belgian government provides a free eID Digital Signature Server[10]. The second is the private sector e-contract service[11]. Both offer signature creation and verification services. Other examples include Trustweaver's verification service[12] for electronic documents. No claim status service providers were implemented.

[10] `https://dss.services.belgium.be`, also `https://sign.belgium.be`

[11] `https://www.e-contract.be/dss`

[12] `https://twa.trustweaver.com/ap/validate.aspx`

Appendix G

List of trusted lists

This appendix provides background information on the European list of trusted lists that was implemented as a consequence of the eIDAS regulation [103].

G.1 Purpose

The List of the Trusted Lists (LOTL) contains the identities of the Trusted List Scheme Operators of by the European Member States and the locations where their Trusted Lists are published. The LOTL is created and maintained by the European Commission.

To quote the European Commission's website[1]: *In order to allow access to the trusted lists of all Member States, the Commission makes available to the public, through a secure channel to an authenticated web server, the trusted lists as notified by Member States, in a signed or sealed form suitable for automated processing.*

The LOTL has its own entry at the trusted list browser[2].

G.2 Availability

The European Commission maintains this list at a publicly communicated location[3]. It serves as an interoperability tool to facilitate the use of national Trusted Lists. The Commission accepts no responsibility or liability whatsoever with regard to the content of national Trusted Lists which lies exclusively with the Member States.

[1] https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

[2] `https://webgate.ec.europa.eu/tl-browser/\#/tl/EU` or `https://esignature.ec.europa.eu/efda/tl-browser/\#/screen/home`

[3] `https://ec.europa.eu/tools/lotl/eu-lotl.xml`

G.3 Formalisation

G.3.1 Standardisation and terminology

The LOTL is created as a trusted list according to ETSI TS 119 612 [89].

G.3.2 Formalisation in XML

The LOTL is a TL, specified in XML version 1 using UTF-8 encoding.

The top-level element of a TL is a *tsl:TrustServiceStatusList*, which contains two elements:

- a *tsl:SchemeInformation* element,
- A *ds:Signature* element.

The *tsl:SchemeInformation* element contains many scheme attributes.

- a TSLType element that identifies it as the EU List of the Lists:

  <TSLType> http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists </TSLType>

- a <*SchemeOperatorName*> element that specifies the European Commission as Scheme Operator
- a <*PointersToOtherTSL*> element, pointing to the Member State TLSOs

The *ds:Signature* contains the signature of the TLSO over the information provided. There is also an encoded *ds:Certificate* element.

Appendix H

Accreditation and conformity assessment

This appendix provides background information on the organisation of accreditation and conformity assesment.

H.1 Introduction

H.1.1 Terminology

Accreditation is a third-party attestation related to a conformity assessment body (such as certification body, inspection body or laboratory) conveying formal demonstration of its competence to carry out specific conformity assessment tasks (such as certification, inspection and testing). An authoritative body that performs accreditation is called an 'accreditation body'.

H.1.2 Global organisation of accreditation

The International Accreditation Forum (IAF) and International Laboratory Accreditation Cooperation (ILAC) provide international recognitions to accreditation bodies. There are many internationally-recognized accreditation bodies approved by the IAF and ILAC.

H.2 Accreditation within Europe

Within the European Economic Area, accreditation is regulated through the Accreditation Regulation [100].

H.2.1 The European co-operation for Accreditation

The European co-operation for Accreditation[1] (EA) is a not-for-profit association, registered in the Netherlands. It is formally appointed by the European Commission in Regulation (EC) No 765/2008 [100] to develop and maintain a multilateral agreement of mutual recognition, the EA MLA, based on a harmonised accreditation infrastructure. The rationale for the authority of the EA can be summarised as follows.

- According to the Regulation, accreditation means an 'attestation by a National Accreditation Body that a Conformity Assessment Body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity'.
- The Regulation identifies the European co-operation for Accreditation (EA) as the sole association entrusted to manage accreditation at European level and defines its responsibilities and obligations in this respect. It places an obligation on EU Member States to accept the results issued by the Conformity Assessment Bodies accredited by any of the EA MLA signatories.
- The EA MLA is recognised[2] at international level by IAF (International Accreditation Forum) and ILAC (International Laboratory Accreditation Cooperation), the two global associations of Accreditation Bodies.

At the time of performing the analysis for the thesis, the first quarter of 2021, the EA had 50 Members. The EA Members are National Accreditation Bodies (NAB) that are officially recognized by their national governments to assess and verify – against international standards – organizations that carry out conformity assessment activities such as certification, verification, inspection, testing and calibration. The European Accreditation publishes its information such as the list of National Accreditation Bodies that are EA members in PDF.

[1] `https://european-accreditation.org/`
[2] `https://european-accreditation.org/mutual-recognition/iaf-ilac-recognition/`

Appendix I

Sources of company data

This appendix provides background information to and a short analysis of public sources of company data that are relevant to the thesis.

I.1 Introduction

Many sources publish data about companies. These include:

- public data sources such as business registers and National Banks, organised on a per country basis,
- EU-wide systems such as
  - the European Business Register Interconnection System (BRIS),
  - the European Data Portal,
- commercial data providers, and
- Linked Open Data sources, referring to data that is both linked and uses open sources.

I.2 Public data sources per country

Information on the identity and selected attributes of companies is available from many sources. There are public data sources that can often be accessed for free.

I.2.1 Business registers

I.2.1.1 Description

Many countries operate a service that can be queried interactively. These include the following:

- the UK's Companies House[1],
- the Belgian Cross-roads database service of the Federal Ministry of Economy[2],
- the Italian InfoCamere[3]
- the Swedish Bolagsverket[4],
- the Spanish Registration Authority[5], the government open data website[6] and the Catalan transparency website[7],
- the German Bundesanzeiger[8],
- the Dutch Kamer van Koophandel[9],
- the French Infogreffe[10].

I.2.1.2 Analysis and interim conclusion

These data sources vary in type of information offered, in language, in format (comma separated value, pdf, XML, ..) and in user interface. Some provide information free of charge, some charge a fee. As a consequence using information from such sources is possible, but limited to specific countries only, and relatively cumbersome.

I.2.2 National Banks

I.2.2.1 Description

In many countries statutory accounts can be submitted electronically to the National Bank in eXtensible Business Reporting Language (XBRL) format. E.g. in Belgium this is possible since 2007[11]. The information is made publicly available by the Balance Sheet department of the Central Bank.

XBRL is used to define and exchange balance sheets and financial statements. As XBRL is XML-based and uses the XML syntax and related XML technologies such as XML Schema,

[1] https://www.gov.uk/government/organisations/companies-house
[2] https://economie.fgov.be/nl/themas/ondernemingen/kruispuntbank-van/diensten-voor-iedereen/kruispuntbank-van-3
[3] http://www.infocamere.it/
[4] http://www.bolagsverket.se/
[5] http://www.registradores.org/
[6] https://datos.gob.es/
[7] https://analisi.transparenciacatalunya.cat
[8] https://www.bundesanzeiger.de/
[9] http://www.kvk.nl/
[10] https://www.infogreffe.fr/societes/
[11] http://www.xbrl.be/

XLink, XPath, and Namespaces, such statutory accounts could be used as data source. One can download the statutory accounts of company from the website of the Belgian Central bank [12], and extract company and auditor records in XBRL format. These can be transformed into RDF that uses the XBRL terms such as $< EntityCurrentLegalName >$ (the official name of the company), $< EntitiyIdentifier >$ (the VAT number) and $< Auditor >$.

I.2.2.2 Analysis and interim conclusion

Statutory accounts are a valuable data source, but with varying types of information offered, in different language, and through different user interfaces. Some provide information free of charge, while others charge a fee. As a consequence using information from such sources is possible, but limited to specific countries only, and relatively cumbersome.

I.2.3 Aggregated public data sources

I.2.3.1 BRIS

The EU-wide Business Register Interconnection System[13] (BRIS) offers an alternative data source. However, these databases and the BRIS are limited to single interactive queries and not in XML format, making it less suitable for the thesis.

I.2.3.2 The European Data Portal

The European Data Portal[14] harvests the metadata of Public Sector Information available on public data portals across European countries. Information regarding the provision of data and the benefits of re-using data is also included. The Open Data used within the European Data Portal is data published by public administrations or on their behalf. The metadata contains the information made available with the data set by the initial publisher. Different licences, or absence of licence may occur and re-uses are invited to check with the owners/publishers of the data what terms and conditions apply to the re-use of the data.

The website of the European Data Portal[15] mentioned it contained 1.217.377 datasets at the time it was analysed as a candidate data source for the thesis.

[12] `http://www.nbb.be.`
[13] `https://e-justice.europa.eu/content\_find\_a_company-489-en.do?clang=en`
[14] `https://www.europeandataportal.eu/en`
[15] `https://www.europeandataportal.eu/en`, last accessed 19 January 2021

I.3 Commercial data sources

Relevant data is sold by companies such as Graydon and Dun & Bradstreet but also made freely available by organisations such as GLEIF. The analysis for the implementation as part of the thesis is limited to data that is freely available.

I.3.1 GLEIF

An introduction to the GLEIF and its ontologies is provided in Appendix D.2.4. GLEIF is particularly relevant for the implementation part of the thesis because it offers the following features.

- GLEIF offers its data as open data as explained on its website[16]. It offers a free search utility[17] and various free download facilities.
- The sources of the GLEIF data can be considered as authoritative. It is based on the use of a globally unique company identifier, the Legal Entity Identifier (LEI). The GLEIF offers a mechanism to correct errors in its records. In case a potential error in LEI data has been identified, the LEI data can be challenged[18].
- GLEIF data is widely used. The LEI Regulatory Oversight Committee publishes an overview[19] of where the use of the LEI has been made mandatory or strongly suggested. This includes most territories worldwide.

I.3.2 GLEIF service providers

There exist many providers of GLEIF related services, including the following.

- There are GLEIF Registration Agents, also referred to as LEI issuers or Local Operating Units (LOUs). These are listed on the GLEIF website[20].
- Although GLEIF makes LEI data freely available, as described in Section D.2.4.4 there are alternative accesses offered for professional users. This includes the Global Market Entity Identifier Utility[21] which is offered by the *Business Entity Data (BED) B.V.* company, a subsidiary of the American financial services company the *Depository Trust & Clearing Corporation (DTCC)*.

[16] `https://www.gleif.org/en/about/open-data`
[17] `https://search.gleif.org/\#/search/`
[18] `https://www.gleif.org//en/lei-data/challenge-lei-data`
[19] `https://www.leiroc.org/lei/uses.htm` last accessed on 19 January 2021
[20] `https://www.gleif.org/en/about-lei/get-an-lei-find-lei-issuing-organizations`
[21] `https://www.gmeiutility.org/`

I.4 Linked Open Data

I.4.1 Description

Linked Open Data offers an alternative to the information sources described above. It combines Linked Data and Open Data as follows.

- *Linked Data* is a term commonly used to refer to data that complies to Tim Berners-Lee's four principles[22] formulated in 2006:

  1. use *uris* as names for things,
  2. use HTTP *uris* so that those names can be looked up,
  3. when a *uri* is looked-up, provide useful information, using the standards (RDF*, SPARQL),
  4. include links to other *uris* so that more things can be discovered.

- *Open Data* is a term commonly used to refer to data that can be freely used and distributed by anyone, subject only to the requirement to attribute and share-alike. There has been a recent increase in the importance of open data, illustrated by the publication of a dedicated EU Directive [102] on open data and the reuse of public sector information.

Linked Open Data refers to data that complies with both terms. It is both linked and uses open sources. There are many publicly available sources of Linked Open Data, including the following.

- Wikipedia[23] and its related data sources (Wikidata, Wikispecies, Wikisource, etc.) as well as DBpedia[24], which makes the Wikipedia data available in a structured way.

- FactForge[25] is a hub of Linked Open Data and articles about people, organisations and locations. It was created by the Bulgarian research company Ontotext as a public data service. Ontotext participated in more than 30 research projects and related initiatives[26]. FactForge represents a large scale public demonstrator of their GraphDB's features.

  The purpose of FactForge is to serve as an index and entry point to the LOD cloud and to present a good use-case for large-scale reasoning and data integration. This is described in the following publications.

[22] `https://www.w3.org/DesignIssues/LinkedData.html`
[23] `https://www.wikipedia.org/`
[24] `https://wiki.dbpedia.org/`
[25] `http://factforge.net`
[26] `https://www.ontotext.com/knowledge-hub/research-projects/`

- Bishop et al. [31] describe the capabilities of FactForge.
- Damova [65] describes how FactForge is made up of central LOD datasets, and how its meta-data, ontologies and reasoning are organised. It includes more than 1 billion data elements from datasets such as DBpedia, Geonames, Wordnet, the Global Legal Entities Identification Foundation (GLEIF) and the Panama Papers.
- Bishop et al. [32] describe how to reason over the data in FactForge.

Particularly the data from the GLEIF is relevant for the thesis, because it includes company information that was obtained from sources that can be considered as authoritative. Entities referred to by LEIs and LEI itself are described in the GLEIF (refer to D.2.4.3) and FIBO (refer to I.4.2.1) ontologies both in natural language and in OWL.

As per its website[27], FactForge contains the *Global Legal Entity Identifier* profiles of about around 3 million organizations, derived from the DTCC *Global Markets Entity Identifier* Utility data dump from 2017.

- The US Library of Congress' Linked Data Service[28] provides interactive and machine access to the Library's authority and bibliographic metadata, along with standards and vocabularies used and/or maintained by the Library of Congress.
- The Linked Open Vocabularies[29] whose main objective is to help publishers and users of linked data and vocabularies to assess what was available, to reuse it, and to insert their own vocabulary production in the ecosystem.

I.4.1.1 Analysis and interim conclusion

Given the type of information available, the way the information is published and relative authority of the different sources, Linked Open Data sources and particularly FactForge's GLEIF data were considered as valid information sources.

I.4.2 Analysis of the FactForge GLEIF data

I.4.2.1 Selection of appropriate FIBO ontology

FIBO Business Entities is structured into ontological modules that each include one or more ontologies. There are eight modules, covering corporations, functional entities, legal entities, ownership and control, partnerships, private limited companies, sole proprietorships, and trusts.

[27] `http://factforge.net/about`, last visited January 3, 2020
[28] `http://id.loc.gov`
[29] `https://lov.linkeddata.es/dataset/lov`

For mapping on the $\mathcal{TE}$ data model, the module *Legal Entities* is relevant because it allows to describe legal entities, which can be used as participants (Functional Service Providers/-Consumers, Endorsers, etc). The module has the abbreviation FIBO-BE-LE. It contains four ontologies:

- Legal Persons,
- Formal Business Organizations,
- Corporate Bodies, and
- LEI entities.

The ontology *Legal Persons* is loadable from the file FIBO_BE_LegalPersons.rdf. This ontology of Legal Persons contains OWL classes such as BusinessEntity, identified by its URI `http://www.omg.org/spec/EDMC-FIBO/BE/LegalEntities/LegalPersons/BusinessEntity`. Further classes include LegalEntity, LegalPerson, NaturalPerson, PowerOfAttorney, Signatory and various more. For every class, a definition in natural language is provided as a *skos:definition*, as well as references to its source (e.g. a dictionary).

The ontology *LEI entities* defines concepts around contractually capable business entities. The terms defined are those which are relevant to the Legal Entity Identifier (LEI) work. The term known as legal entity in that work is identified as a formal organization which is recognized in some jurisdiction as being *capable of incurring some liability*, whether or not is a legal person as understood by the legal community. This is labelled as contractually capable entity, to avoid confusion with the accepted legal term for Legal Entity. Such entities are recognized as requiring an LEI, but the identifier itself is allocated to the formal organization which is recognized as being contractually capable.

The ontology has the abbreviation *fibo-be-le-lei* and is loadable from the file *FIBO_BE_LEIEntities.rdf*. Its classes are *ContractuallyCapableEntity, LegalEntity, LegalEntityIdentifier, LegalEntityIdentifierScheme*, and some deprecated classes (*MuncipalEntity, Sovereign, SupranationalEntity*). It has the property *hasAddressOfLegalFormation*.

The two remaining ontologies (*Formal Business Organizations* and *Corporate Bodies*) contain complementary information.

I.4.2.2 Identification of classes and properties

The ontology *fibo-be-le-lei* has the classes *LegalEntity* and *LegalEntityIdentifier*. The class *LegalEntity* is a subclass of AutonomousAgent / LegalPerson. Definition of the class LegalEntity is *isOrganizedIn exactly one Jurisdiction* and *LegalPerson*. The ontology is stored under the file name FIBO_BE_LegalPersons.rdf, abbreviated to fibo-be-le-lp.

The following properties can be identified by using the the FactForge SPARQL endpoint[30].

- Four properties of *LegalEntityIdentifier*can be listed by the query described in Listing I.3. These properties are:
  - rdf:type,
  - fibo-fnd-aap-agt:identifies,
  - fibo-fnd-arr-id:isIndexTo,
  - fibo-fnd-rel-rel:hasUniqueIdentifier.
- Additional properties of *LegalEntity* can be listed by submitting the query described in Listing I.1.
- Additional properties of *LegalPerson* can be listed by submitting the query described in Listing I.2.

Listing I.1: FactForge query for LegalEntity properties

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX fibo-be-le-lp: <http://www.omg.org/spec/EDMC-FIBO/BE/LegalEntities/LegalPersons/>
SELECT DISTINCT ?property
WHERE { ?indiv rdf:type fibo-be-le-lp:LegalEntity;
               ?property ?value. }
```

Listing I.2: FactForge query for LegalPerson properties

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX fibo-be-le-lp: <http://www.omg.org/spec/EDMC-FIBO/BE/LegalEntities/LegalPersons/>
SELECT DISTINCT ?property
WHERE { ?indiv rdf:type fibo-be-le-lp:LegalPerson;
               ?property ?value. }
```

Listing I.3: FactForge query for LegalEntityIdentifier properties

```
WHERE { ?indiv rdf:type fibo-be-le-lei:LegalEntityIdentifier ;
               ?property ?value. }
```

As per the FIBO Foundations specification, the *fibo-fnd-aap-agt:identifies* is a property of the class AutonomousAgent. It is the relationship between something and that which provides a unique reference for it. Its inverse is *isIdentifiedBy*, which can be used by queries such as described in Listing I.4.

[30] `http://factforge.net/sparql`

Listing I.4: FactForge query that uses isIdentifiedBy

```
SELECT ?indiv ?name ?identifier
WHERE {?indiv rdf:type fibo-be-le-lp:LegalEntity;                                    fibo
      -fnd-aap-agt:isIdentifiedBy ?identifier ;                                  fibo-fnd-aap
      -agt:hasName ?name. }
```

I.5 Conclusion

On the basis of the preceding analysis, the Linked Open Data source *FactForge* and its GLEIF data was selected as data source for information about companies.

Appendix J

Sources of natural person information

This appendix provides background information on, and an analysis of, available information regarding natural persons. The focus of the descriptions is on what is most relevant to the thesis.

J.1 Introduction

First and foremost, personal data of natural persons is protected in Europe by the General Data Protection Regulation [101]. This imposes limitations on what can be done with personal data, and how it must be protected in cases where its usage is allowed. Taking these limitations into consideration, this appendix analyses three types of candidate information sources related to natural persons.

- Section J.2 analyses public sources.
- Section J.3 analyses private sources.
- Section J.4 analyses self-published sources.

J.2 Analysis of candidate public data sources

In the public sector, information about citizens and residents is kept and used by their governments.

J.2.1 Examples of country data sources

Countries are sovereign in their organisation of such information, which includes the use of information repositories, identity attributes and the use of one or more numbers for identification purposes. As a consequence, the systems that are in use diverge widely.

An authoritative overview of official identity documents is provided as the Public Register of Authentication Documents On-line (PRADO) by the European Consillium[1]. The register covers EU Member States as well as other states. Each identity document is described, and when a national identification number is printed on a document, it is shown. An overview of the national identification numbers is not provided.

Wikipedia[2] provides a non-authoritative global overview. The following cases are provided as examples only.

- In some countries, the government oversees private sector entities they allow to manage on-line identities and credentials for public and private sector use. Examples of this approach include the United Kingdom and Italy.
  - The UK system, *Gov.UK Verify*[3], is described by Tsakalakis et al [315].
  - The Italian system, Sistema Pubblico di Identita Digitale (SPID), is documented on its website[4].
- Other countries establish a national governmental identity management system that is mandatory for all inhabitants, with a dedicated entity that collects, stores and manages identity and biometric data in a single system.
  - The Indian 'National Register of Citizens (NRC)' is a relevant example. It is a mandatory register of all Indian citizens whose creation was mandated by the 2003 amendment of the Citizenship Act, 1955[5]. India also established the Unique Identification Authority of India[6] (UIDAI), whose Aadhaar system is arguably the world's largest biometric ID system.
  - At a smaller scale, the Belgian National Identity Register[7] provides similar services. Each citizen and each resident is described in a set of database records and uniquely identified by a national registration number. Regarding electronic identification and authentication, the following can be observed.

[1] `https://www.consilium.europa.eu/prado/en/prado-start-page.html`

[2] `https://en.wikipedia.org/wiki/National_identification_number`

[3] Described at `https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify`

[4] `https://www.spid.gov.it/`

[5] See `https://www.refworld.org/pdfid/410520784.pdf`, where Section 14A on the issue of national identity cards states: (l) The Central Government may compulsorily register every citizen of India and issue national identity card to him. (2) The Central Government may maintain a National Register of Indian Citizens and for that purpose establish a National Registration Authority.

[6] `https://uidai.gov.in/`

[7] `https://www.ibz.rrn.fgov.be/nl/rijksregister/`

* Regarding certificates, Certipost was selected by the government as Trust Service Provider for operating the X.509-based PKI that supports the identity register by issuing authentication and signature certificates. Citizen certificates are signed by the Certipost CitizenCA, which is a sub-CA of the Belgian Root CA. The responsibilities of Certipost are described on-line on the website of the national identity register[8] and in the Certipost Certification Practise Statement[9]. Furthermore:
  - There are no public registers of citizen certificates available. Citizen certificates are stored on the electronic identity card can be read and exported from there.
  - The private keys are generated and stored within the identity card, and can only be used after authentication of the card-holder by the Java applet on the card, using a four-digit PIN code.
  - The national registration number is printed on the backside of the identity card. Its usage is forbidden unless approval was obtained from the Privacy Commission.
* Regarding on-line electronic authentication, the Belgian Federal Public Service *Digital Transformation*[10] offers a Federal Authentication Service[11] (FAS) for access to government applications. This service authenticates citizens and residents. The service allows a government application to delegate the authentication to the FAS server which can produce a SAML [259] or OIDC [267] token containing the citizen or resident's name and national register number upon successful authentication with the national identity card. This authentication requires the card to sign a random challenge from the FAS with its private key.
  - As described in the FAS Cookbook [115], in case of a SAML token the FAS generates a signed and base64[12] encoded SAML response. The response contains an assertion with the attribute 'issuer', which will have the value '`http://www.belgium.be`' and an *AuthenticationStatement* element, which will contain the national register number.
  - As described in the FAS OIDC Onboarding manual [85], in case of OIDC

[8] `https://www.ibz.rrn.fgov.be/nl/identiteitsdocumenten/eid/aansprakelijkheden/`
[9] `https://repository.eid.belgium.be/downloads/citizen/nl/CPS_CitizenCA.pdf`
[10] `https://dt.bosa.be/en`
[11] `https://dt.bosa.be/en/identificatie_beveiliging/federal_authentication_service`
[12] Base64 is a group of binary-to-text encoding schemes that represent binary data (more specifically a sequence of 8-bit bytes) in an ASCII string format by translating it into a radix-64 representation. It is designed to carry data stored in binary formats across channels that only reliably support text content.

the FAS generates a signed access token response which contains an id-token. Inside the id-token there is the subject's national register number or email address. The id-token is signed by the FAS' authorisation server.

The token is communicated to the end-user's browser, for forwarding to the application. The token can be intercepted by the browser and corresponds to a $\mathcal{TE}$ identity attestation issued by the Federal Public Service.

- Austria protects the identification number of its citizens and residents by using unlinkable sector-specific personal identifiers. It created a system with sector-specific identifiers that are derived from a source personal identification number (SourcePIN). The country operates a Central Register of Residents (CRR), where each resident has a unique number (referred to as 'ZMR-Zahl' or 'Stammzahl'). Parallel to this central register, there exist other registers which identify residents using their own numbers. These include the Commercial Register, the Register of Associations, and the Supplemental Registers for citizens not enrolled in the CRR (e.g. expatriates, foreigners).

  The SourcePIN Register Authority operates under supervision of the Data Protection Commission and creates a SourcePIN for each resident on the basis of the unique identifiers in the different registers. It is stored encrypted at the register. Residents are not identified by their SourcePIN, but by a sector-specific PIN. Sectors (healthcare, taxation, finance, ...) have a sector identifier. The SourcePIN Register Authority combines a resident's SourcePIN with a sector identifier to create a sector-specific PIN. As this is based on a cryptographic hash, the SourcePIN cannot be derived from the sector-specific PIN. The Austrian Citizen Card stores an XML data structure that holds name, date of birth, the base64 encoded SourcePIN[13] and the public keys of the certificates signed by the authority. The Citizen Card is implemented in various ways and can be used for on-line authentication and signature. The generated tokens corresponds to a $\mathcal{TE}$ identity attestation issued by the Austrian government.

- The Netherlands use the BSN[14] as identifier. Polymorph encrypted pseudonyms, described by Verheul et al. [329], can replace the BSN in a number of on-line authentication use cases. Verheul [328] describes the use of such pseudonyms in context of electronic identity. The system is based on the homomorphic properties of ElGamal encryption. It adds a pseudonym provider, a key management authority and law enforcement point for identity investigation to the traditional roles of end-user, identity provider and service provider. The functioning can be summarised as follows.

[13] See the description at `https://www.buergerkarte.at/konzept/personenbindung/spezifikation/20050214/`

[14] BSN goes back to the terms 'Burger Sofi Nummer', which can be loosely translated as 'citizen social financial number'.

- The key management authority provides the pseudonym provider with a specific public key for each identity provider, and provides each identify provider with a specific public key for the service providers.
- End-user registration is performed as follows.
  * An end-user registers with an identity provider that compiles a system-wide user identifier *U-id* for the user.
  * The identity provider sends this *U-id* to the pseudonym provider, and receives a polymorphic pseudonym that is stored for later use.
- When an end-user wants to use the services of a service provider, the end-user authenticates with the identity provider. Upon successful authentication, the identity provider encrypts the pseudonym with the service provider's key, and transmits the result to the service provider. The service provider can recover the pseudonym and relies on the identity provider for having performed the authentication of the end-user.
- The law enforcement point for identity investigation handles two requests.
  * 'De-pseudonymisation' when an encrypted pseudonym and the service provider where it was used are presented, and the pseudonym is transformed back into the user identity. This allows the handling of complaints about user-fraud.
  * 'Pseudonymisation on request' when a user identity is presented and transformed into pseudonyms for one or more service providers. This allows investigations such as e.g. child grooming, where law enforcement wants to evaluate whether an identity has been active on other services or websites as well.

Such an encrypted pseudonym corresponds to a $\mathcal{TE}$ identity attestation issued by an identity provider.

For cross-border identification the following systems were identified.

- The international system of apostilles, based on the international treaty drafted by the Hague Conference on Private International Law [144] allows to give legal value to public documents. This includes administrative documents such as birth certificates. The objective of the convention is to allow an originating state to make a public document available to a destination state. At the end of 2020 there were 119 participating countries[15] which operate Competent Authorities to issue apostilles. In 2006 the electronic

[15]Last retrieved on 30/12/2020 from `https://www.hcch.net/en/instruments/conventions/status-table/`

apostille was launched, containing apostilles in electronic format with a digital certificate, and on-line registers that allow to verify the original document and the electronic apostille. The registers are used to record the particulars of all apostilles issued by the Competent Authority (i.e. paper and electronic apostilles). To avoid misuse, registers only allow access to persons who have actually received an apostille and want to verify its issuance.

- A number of European Member States use the personal data kept at national level to support cross-border identification and authentication. This is done via the so-called eIDAS nodes which act as proxy identity servers which reroute requests to the 'home'-identity service provider of the person that wants to be identified or authenticated. An analysis is provided in the next section, Appendix J.2.2.

J.2.2 Examples within eIDAS jurisprudence

J.2.2.1 Core Person Vocabulary

To define the semantics of the identity data for cross-border use within the European Union, the European Commission specified a Core Person Vocabulary. This is one of the Core Vocabularies that were created to promote interoperability. The set of Core Vocabularies can be downloaded from the Joinup website[16]. The 'Core Person Vocabulary' defines the following attributes for a natural person.

- full name,
- given name,
- family name,
- patronymic name,
- alternative name,
- gender,
- birth name,
- date of birth,
- date of death,
- country of birth,

[16] `https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies`

- country of death,
- place of birth,
- place of death,
- citizenship,
- residency,
- jurisdiction,
- identifier.

J.2.2.2 eIDAS eID Profile

The Core Person Vocabulary is used in the eIDAS identity profile. The profile is used between identity providers and eIDAS nodes (which serve as a gateway in cross-border on-line authentication). The profile is available from the Connecting Europe Facility[17] and consists of the following four documents.

- eIDAS Message Format [82]
- eIDAS Interoperability Architecture [81]
- eIDAS Cryptographic Requirement [80]
- eIDAS SAML Attribute Profile [83]

The SAML Attribute Profile describes the mapping of the semantic definitions of the Core Person Vocabulary onto the SAML protocol fields.

Cross-border unique identifier For cross-border identification, Implementing Regulation 2015/1501 establishes that the minimum data set for a natural or legal person shall contain a unique identifier (besides name, surname and birth date for a natural person, and besides the legal name for a legal person). According to the eIDAS technical specifications, the unique identifier is composed as follows:

- The first part is the Nationality Code of the identifier. This is one of the ISO 3166-1 alpha-2 codes, followed by a slash ('/').
- The second part is the Nationality Code of the destination country or international organization. This is one of the ISO 3166-1 alpha-2 codes, followed by a slash ('/').

[17] `https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile`

- The third part is a combination of readable characters. This uniquely identifies the identity asserted in the country of origin but does not necessarily reveal any correspondence with the subject's actual identifier in the country of origin.

'ES/AT/02635542Y' is an example of a Spanish eIDNumber for cross-border use by an Austrian Service Provider.

J.2.3 Interim conclusion

J.2.3.1 Regarding the use of country-specific data

It was concluded that the information in the data sources described in Section J.2.1 is regulated and in general not publicly available. These data sources offer only limited data that could be used for the $\mathcal{TE}$ model implementation. The use of such data was limited to the demonstration that a citizen certificate issued under the authority of a national identity register can be used to create an identity attestation. This demonstration was based on a Belgian citizen certificate.

J.2.3.2 Regarding the use of eIDAS-wide data

It was concluded that the use of the cross-border unique identifiers and of the eIDAS nodes described in Section J.2.2 is regulated and not publicly available. As a consequence these data sources do not offer data that could be used for the $\mathcal{TE}$ model implementation.

J.3 Analysis of candidate private sources

J.3.1 Description

As for the European public sector, the collection and processing of personal data by the private sector is subject to the General Data Protection Regulation [101]. Regarding electronic data sources, the following can be observed.

- Some private sector companies offer identity checks against payment in the context of employment or 'know your customer' procedures. This typically requires contractual arrangements to be in place.
- Identity enrolment in the private sector[18] identity management systems leads to having citizen's identity attributes available and their authentication being supported by such systems. However neither the attributes nor the authentication are available unless contractual arrangements are in place.

[18]Such enrolment may require the demonstration of a government-issued credential, particularly in sectors such as financial services.

J.3.2 Interim conclusion

As a consequence it was concluded that these private data sources do not offer data that could be used for the $\mathcal{TE}$ model implementation.

J.4 Self-published data

Self-published data can be classified as a sub-domain of private data sources. The following sources were identified:

- PGP's web of trust,
- W3C's Verifiable Credentials,
- Schema.org's vocabulary,
- FOAF data sets.

J.4.1 PGP's web of trust

In the web of trust created by PGP, participants generate their public key and identity attributes, and make this information publicly available through key servers. However, the web of trust model suffers from lack of clarity regarding its semantics, as described in Section 6.2.1. Therefore it was decided not to use it as a data source.

J.4.2 W3C's Verifiable Credentials

The W3C published the 'Verifiable Credential Data Model 1.0 specification' [378]. A Verifiable Credential (VC) is defined as 'a tamper-evident credential that has authorship that can be cryptographically verified'. Verifiable Credentials present an abstract data model for claims, which are a list of attributes and values pertaining to a subject. Such a claim is created by an issuer who then creates a verifiable credential, which in turn is processed by a verifier. To identify the subject of Verifiable Credentials, the W3C specified 'Decentralized Identifiers (DIDs)' [379]. W3C VCs and DIDs are used in the Solid architecture, proposed by Berners-Lee [232].

Halpin [141] analysed the security of Verifiable Credentials and concluded they are vulnerable to signature exclusion and signature replacement attacks where an adversary can remove the signature of a signed message, replace it with another signature, and trick the verifier into falsely accepting the message as valid due to ambiguity in parsing.

As the software implementation of the Solid components and of VC and DID building blocks is still work in progress, it was concluded that DID and VC-based data sources do not (yet) offer data that could be used for the $\mathcal{TE}$ model implementation.

J.4.3 Schema.org

The Schema.org community promotes schemas for structured data on the Internet. The community was founded by Google, Microsoft, Yahoo and Yandex, and there is participation by the larger Web community. Since April 2015, the W3C Schema.org Community Group is the main forum for schema collaboration. See Krutil [209] for a description of how Schema.org's vocabulary is used for the classification of web pages. As the purpose of the Schema.org vocabularies is search engine optimisation it was concluded that data sources that make use of this vocabulary do not offer data that is relevant to the $\mathcal{TE}$ model implementation.

J.4.4 FOAF

The Friend of a Friend (FOAF) specification aimed to create a linked information system. The FOAF Vocabulary Specification [37] defines a dictionary of people-related terms that can be used in structured data. The following evidence of its use was identified.

- A description of FOAF's usage on the semantic web is provided by Ding et al. [73].
- The W3C publishes a list of sites[19] that maintain FOAF records of their users.
- According to the data published by the Ontology Engineering Group of the Madrid Politechnical University[20] it is used in 249 data sets.
- A search on Elsevier's Mendeley Data Search[21] returned 34 FOAF data sets. These include aggregated data sets.
- Kalemi and Martiri [194] proposed a dedicated FOAF ontology for academic use, FOAF-Academic.
- For a recent extension in the context of public health see Amith et al. [6].

J.4.5 Interim conclusion

As multiple FOAF data sets are available in RDF format, such data sets can be chosen as a data source for the $\mathcal{TE}$ model implementation. It was decided to use an aggregated FOAF file from Mendeley Data Search because such a file contains information that can be mapped onto $\mathcal{TE}$ model predicates. The evaluation of this information is further described in Table 12.6.

[19] `https://www.w3.org/wiki/FoafSites`

[20] `https://lov.linkeddata.es/dataset/lov/vocabs/foaf`, last accessed on 5/1/2021.

[21] Using `https://data.mendeley.com/research-data/?type=DATASET&search=foaf`, performed on 6/1/2021.

Appendix K

Transformation source code

This appendix provides examples of transformations used as part of the implementation of the $\mathcal{TE}$ framework. Illustrations of both the XSL transformation and the Java code that drives it are provided.

K.1 Data sources

As an illustration, the XSL transformation that creates the DataSource instance on the basis of the Belgian trusted list is described in Listing K.1. The Java code that invokes it is described in Listing K.2. Further sources can be found on-line[1].

Listing K.1: TL2RDF_BE_DataSource_TL_v301.xsl

```
1  <?xml version="1.0"?>
2  <!--
3  Name: TL2RDF_BE_DataSource_TL_v301.xsl
4
5  Purpose:
6  Creation of data sources from on-line trusted list publications
7
8  Description:
9  XSLT script to create data sources as instances of the te:DataSource class
10
11 The on-line trusted lists on which those instances are based:
12  * Belgium https://tsl.belgium.be/tsl-be.xml
13  * Italy https://eidas.agid.gov.it/TL/TSL-IT.xml
14  * Spain https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml
15  * United Kingdom https://www.tscheme.org/sites/default/files/tsl-uk0022signed.xml
16
17 After execution
18 * OWL must be selected from output file using a browser, NOT a text editor (to preserve the less than greater than
       sign)
19 * Should any "<_" (blank after < ) or "_>" (blank before >) remain they must be replaced by "<" or ">"
20
21 Step 0 Creation of the activity that generates the data source
22
```

[1]They can be found at `http://www.marcsel.eu/ti/xsl/NAME.xsl` by replacing NAME with the name of the desired transformation

```
23  S0.1 create resource with hardcoded name based on xsl and its execution
24  S0.2 cast into type of prov:Activity
25  S0.3 add startedAtTime
26  S0.4 add endedAtTime
27
28  Step 10 Creation of DataSource individuals
29
30  S10.1 create resource with hardcoded name based on official uri
31  S10.2 cast into type of te:DataSource
32  S10.3 add wasDerivedFrom the online TL
33  S10.4 add wasAttributedTo the TLSO
34  S10.5 add wasGeneratedBy the .xsl program
35
36  Author: Marc Sel
37  Date 20/12/2020 last updated 08/01/2021
38
39  -->
40  <xsl:stylesheet version="1.0"
41              xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
42              xmlns:html="http://www.w3.org/1999/xhtml"
43              xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
44              xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
45              xmlns:dcterms="http://purl.org/dc/terms"
46                          xmlns:owl="http://www.w3.org/2002/07/owl#"
47                          xmlns:prov="http://www.w3.org/ns/prov#"
48                          xmlns:fn="http://www.w3.org/2005/xpath-functions"
49                          xmlns:te="http://www.marcsel.eu/onto/te/"
50              xmlns:foaf="http://xmlns.com/foaf/spec/"
51              xmlns:tsl="http://uri.etsi.org/02231/v2#">
52
53  <xsl:template match="tsl:SchemeOperatorName">
54  <!-- Variables -->
55  <!-- VAR-NAME-RULEBOOK selects rulebook name, for which the URI is used because some scheme operators provide
        whole sections of text in the name field -->
56  <!-- all on single line -->
57  <xsl:variable name="VAR-NAME-RULEBOOK"><xsl:value-of select="/tsl:TrustServiceStatusList/tsl:SchemeInformation/tsl
        :SchemeInformationURI"/></xsl:variable>
58  <!-- <xsl:copy-of select="$VAR-NAME-RULEBOOK"/>  -->
59
60  <!-- VAR-NAME-TLSO selects TLSO name -->
61  <!-- all on single line -->
62  <xsl:variable name="VAR-NAME-TLSO"><xsl:value-of select="tsl:Name"/></xsl:variable>
63  <!-- <xsl:copy-of select="$VAR-NAME-TLSO"/>  -->
64
65  <!-- VAR-100 generates the < sign -->
66  <!-- all on single line -->
67  <!-- attempt to replace &lt; by &lt results in error msg: the reference to entity "lt" must end with the ';'
        delimiter.-->
68  <xsl:variable name="VAR-100">&lt;</xsl:variable>
69  <!-- <xsl:copy-of select="$VAR-100"/> -->
70
71  <xsl:variable name="VAR-200"><xsl:value-of select="tsl:Name"/></xsl:variable>
72  <!-- <xsl:copy-of select="$VAR-200"/> -->
73
74  <!-- VAR-900 generates the > sign -->
75  <xsl:variable name="VAR-900">&gt;</xsl:variable>
76  <!-- <xsl:copy-of select="$VAR-900"/> -->
77
78  <owl:NamedIndividual>
79  <!-- S0  creation of the activity that generates the data source -->
80  <!-- S0.1 create resource with hardcoded name based on xsl and its execution-->
81  <xsl:attribute name="rdf:about">_http://www.marcsel.eu/ti/xsl/TL2RDF_BE_DataSource_TL_v301.xsl.2021-01-06</xsl:
        attribute>
82  <xsl:text>&#10;</xsl:text>
83  <xsl:comment>TL2RDF_DataSource_TL_v301_S0_1 NamedIndividual Activity created </xsl:comment>
84  <xsl:text>&#10;</xsl:text>
85
86  <!-- S0.2 cast into type of prov:Activity  -->
87  <rdf:type rdf:resource="http://www.w3.org/ns/prov#Activity"/>
88  <xsl:text>&#10;</xsl:text>
89  <xsl:comment>TL2RDF_DataSource_TL_v301_S0_2 NamedIndividual cast into type prov:Activity </xsl:comment>
90  <xsl:text>&#10;</xsl:text>
```

```
91
92  <!-- S0.3 add startedAtTime -->
93  <prov:startedAtTime rdf:datatype="http://www.w3.org/2001/XMLSchema#dateTime">2021-01-06T22:33:52</prov:
        startedAtTime>
94  <xsl:text>&#10;</xsl:text>
95  <xsl:comment>TL2RDF_DataSource_TL_v301_S0_3 add property startedAtTime</xsl:comment>
96  <xsl:text>&#10;</xsl:text>
97
98  <!-- S0.4 add endedAtTime -->
99  <prov:endedAtTime rdf:datatype="http://www.w3.org/2001/XMLSchema#dateTime">2021-01-06T22:33:52</prov:endedAtTime>
100 <xsl:text>&#10;</xsl:text>
101 <xsl:comment>TL2RDF_DataSource_TL_v301_S0_4 add property endedAtTime</xsl:comment>
102 <xsl:text>&#10;</xsl:text>
103
104 </owl:NamedIndividual>
105
106 <owl:NamedIndividual>
107 <!-- S10 creation of the data source -->
108 <!-- S10.1 create resource with hardcoded name based on official uri-->
109 <xsl:attribute name="rdf:about">_https://tsl.belgium.be/tsl-be.xml</xsl:attribute>
110 <xsl:text>&#10;</xsl:text>
111 <xsl:comment>TL2RDF_DataSource_TL_v301_S10_1 NamedIndividual created </xsl:comment>
112 <xsl:text>&#10;</xsl:text>
113
114 <!-- S10.2 cast into type of DataSource -->
115 <rdf:type rdf:resource="http://www.marcsel.eu/onto/te/DataSource"/>
116 <xsl:comment>TL2RDF_DataSource_TL_v301_S10_2 NamedIndividual cast into type te:DataSource </xsl:comment>
117 <xsl:text>&#10;</xsl:text>
118
119 <!-- S10.3 add wasDerivedFrom -->
120 <!-- Name of data source is hardcoded -->
121 <prov:wasDerivedFrom rdf:resource="https://tsl.belgium.be/tsl-be.xml"/>
122 <xsl:comment>TL2RDF_DataSource_TL_v301_S10_3 wasDerivedFrom </xsl:comment>
123 <xsl:text>&#10;</xsl:text>
124
125 <!-- S10.4 add wasAttributedTo agent -->
126 <xsl:copy-of select="$VAR-100"/>prov:wasAttributedTo rdf:resource="http://www.marcsel.eu/ti"/>"/<xsl:copy-of_
        select="$VAR-900"/>
127 <xsl:comment>TL2RDF_DataSource_TL_v301_S10_4_wasAttributedTo_</xsl:comment>_____
128 <xsl:text>&#10;</xsl:text>_____
129
130 <!--_S10.5_add_wasGeneratedBy_activity_-->
131 <prov:wasGeneratedBy_rdf:resource="_http://www.marcsel.eu/ti/xsl/TL2RDF_BE_DataSource_TL_v301.xsl.2021-01-06"/>
132 <xsl:comment>TL2RDF_DataSource_TL_v301_S10_5 wasGeneratedBy</xsl:comment>
133 <xsl:text>&#10;</xsl:text>
134
135 </owl:NamedIndividual>
136
137 </xsl:template>
138
139 <xsl:template match="/">
140 <xsl:text>&#10;</xsl:text>
141 <rdf:RDF>
142 <xsl:text>&#10;</xsl:text>
143 <xsl:apply-templates select="/tsl:TrustServiceStatusList/tsl:SchemeInformation/tsl:SchemeOperatorName"/>
144 <xsl:text>&#10;</xsl:text>
145 </rdf:RDF>
146 <xsl:text>&#10;</xsl:text>
147 </xsl:template>
148
149 </xsl:stylesheet>
```

Listing K.2: XSL TL2RDF_BE_DataSource_TL_v301.java

```
1
2  package ti_package;
3
4  /
```

```
5     @author selm
6     Date 18/12/2019 last updated 17/12/2020
7      /
8   import java.io.FileNotFoundException;
9   import java.io.FileOutputStream;
10  import java.io.IOException;
11
12  import javax.xml.transform.Transformer;
13  import javax.xml.transform.TransformerConfigurationException;
14  import javax.xml.transform.TransformerException;
15  import javax.xml.transform.TransformerFactory;
16  import javax.xml.transform.stream.StreamResult;
17  import javax.xml.transform.stream.StreamSource;
18
19  import org.apache.xalan.trace.PrintTraceListener;
20  import org.apache.xalan.trace.TraceManager;
21  import org.apache.xalan.transformer.TransformerImpl;
22
23  public class TL2RDF_BE_DataSource_TL_v301 {
24  public static void main(String[] args) throws TransformerException,
25                          TransformerConfigurationException, FileNotFoundException,
26                          IOException, java.util.TooManyListenersException,
27                          org.xml.sax.SAXException
28  {
29  // program name
30  String program_name ="TL2RDF_BE_DataSource_TL_v301";
31
32  // Files used
33  String input_1_XSL = "C:/Users/Sel/Documents/Sierra/eclipse-workspace-mars1-TI/TI/xsl/TL2RDF_BE_DataSource_TL_v301
        .xsl";
34  String input_2_XML = "C:/Users/Sel/Documents/Sierra/eclipse-workspace-mars1-TI/TI/xml/ts1-be.20201217.xml";
35  String output_1_LOG = "C:/Users/Sel/Documents/Sierra/eclipse-workspace-mars1-TI/TI/log/
       TL2RDF_BE_DataSource_TL_v301.log";
36  String output_2_RDF = "C:/Users/Sel/Documents/Sierra/eclipse-workspace-mars1-TI/TI/rdf/
       TL2RDF_BE_DataSource_TL_v301.rdf";
37
38  // 1 Set up a PrintTraceListener object to print to a file.
39  java.io.FileWriter fw =
40          new java.io.FileWriter(output_1_LOG);
41  java.io.PrintWriter pw = new java.io.PrintWriter(fw, true);
42  PrintTraceListener ptl = new PrintTraceListener(pw);
43
44  // 2 Print information as each node is 'executed' in the stylesheet.
45  ptl.m_traceElements = true;
46  // Print information after each result-tree generation event.
47  ptl.m_traceGeneration = true;
48  // Print information after each selection event.
49  ptl.m_traceSelection = true;
50  // Print information whenever a template is invoked.
51  ptl.m_traceTemplates = true;
52  // Print information whenever an extension call is made.
53  ptl.m_traceExtension = true;
54
55  // 3 Instantiate factory
56  TransformerFactory tFactory = TransformerFactory.newInstance();
57
58  // 4 Create transformer from xsl
59  Transformer transformer = tFactory.newTransformer(
60          new StreamSource(input_1_XSL));
61          System.out.println(program_name + "-101_Input_1_XSL_is_in_" + input_1_XSL);
62
63  // 5 Run xsl transformer on xml
64  // Cast the Transformer object to TransformerImpl.
65  if (transformer instanceof TransformerImpl) {
66          TransformerImpl transformerImpl = (TransformerImpl) transformer;
67          TraceManager trMgr = transformerImpl.getTraceManager();
68          trMgr.addTraceListener(ptl);
69
70  // Perform the transformation --printing information to
71  // the events log during the process.
72  System.out.println(program_name + "-102_Input_2_XML_is_in_" + input_2_XML);
73
```

```
74  transformer.transform(
75          new StreamSource(input_2_XML),
76          new StreamResult(new FileOutputStream(output_2_RDF)));
77  }
78  // Close the PrintWriter and FileWriter.
79  pw.close();
80  fw.close();
81
82  System.out.println(program_name + "-103_Output_1_LOG_is_in_" + output_1_LOG );
83  System.out.println(program_name + "-104_Output_2_RDF_is_in_" + output_2_RDF);
84  }
85  }
```

K.2 Trustworthiness monitor

As an illustration, the XSL transformation that creates the trustworthiness monitor on the basis of the Belgian trusted list is provided below. As the Java code only differs from the one used for the creation of the data sources in the names of the input and output files, it is not repeated.

Listing K.3: TL2RDF_BE_TwsMo_v301.xsl

```
1   <?xml version="1.0"?>
2   <!--
3   Name: TL2RDF_BE_TwsMo_v301.xsl
4
5   Purpose:
6   Creation of trustworthiness monitors from on-line trusted list publications
7
8   Description:
9   XSLT script to create trustworthiness monitors as organisations with a TwsMo role attestation
10
11  The on-line trusted lists on which those instances are based:
12   * Belgium https://tsl.belgium.be/tsl-be.xml
13   * Italy https://eidas.agid.gov.it/TL/TSL-IT.xml
14   * Spain https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml
15   * United Kingdom https://www.tscheme.org/sites/default/files/tsl-uk0022signed.xml
16
17  After execution
18  * OWL must be selected from output file using a browser, NOT a text editor (to preserve the less than greater than
        sign)
19  * Should any "<_" (blank after < ) or "_>" (blank before >) remain
20    they must be replaced by "<" or ">"
21
22  Step 1 Creation of identities for TwsMo and attestations
23
24    S10 creation of identity for TwsMo
25    S11 creation of identity for identity attestation
26    S12 creation of identity for role attestation as TwsMo
27
28  Step 2 Creation of attestations
29
30    S20 creation of identity attestation _IdentityAttestation_FOD_Eco
31    S21 creation of role attestation TwsMo
32
33  Step 3 Creation of TwsMo individual
34
35   S30 creation of TwsMO based on TL TLSO
36
37      allocate identity and attestations,
38      give name, relate to its own identity,
39      cast into type of org:Organization and prov:Organization,
40      self-attest identity,
41      self-attest TwsMo role
```

```
42      add provenance: wasDerivedFrom, wasGeneratedBy, wasAttributedTo
43
44  Author: Marc Sel
45  Date 18/12/2019 last updated 22/12/2020
46
47  -->
48  <xsl:stylesheet version="1.0"
49                  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
50                  xmlns:html="http://www.w3.org/1999/xhtml"
51                  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
52                  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
53                  xmlns:dcterms="http://purl.org/dc/terms"
54                              xmlns:owl="http://www.w3.org/2002/07/owl#"
55                              xmlns:prov="http://www.w3.org/ns/prov#"
56                              xmlns:te="http://www.marcsel.eu/onto/te/"
57                  xmlns:foaf="http://xmlns.com/foaf/spec/"
58                  xmlns:tsl="http://uri.etsi.org/02231/v2#">
59
60  <xsl:template match="tsl:SchemeOperatorName">
61  <!-- Variables -->
62  <!-- VAR-NAME-RULEBOOK selects rulebook name, for which the URI is used because some scheme operators provide
        whole sections of text in the name field -->
63  <!-- all on single line -->
64  <xsl:variable name="VAR-NAME-RULEBOOK"><xsl:value-of select="/tsl:TrustServiceStatusList/tsl:SchemeInformation/tsl
        :SchemeInformationURI"/></xsl:variable>
65  <!-- <xsl:copy-of select="$VAR-NAME-RULEBOOK"/> -->
66
67  <!-- VAR-NAME selects TLSO name -->
68  <!-- all on single line -->
69  <xsl:variable name="VAR-NAME-TLSO"><xsl:value-of select="tsl:Name"/></xsl:variable>
70  <!-- <xsl:copy-of select="$VAR-NAME-TLSO"/> -->
71
72  <!-- VAR-100 generates the < sign -->
73  <!-- all on single line -->
74  <!-- attempt to replace &lt; by &lt results in error msg: the reference to entity "lt" must end with the ';'
        delimiter.-->
75  <xsl:variable name="VAR-100">&lt;</xsl:variable>
76  <!-- <xsl:copy-of select="$VAR-100"/> -->
77
78  <xsl:variable name="VAR-200"><xsl:value-of select="tsl:Name"/></xsl:variable>
79  <!-- <xsl:copy-of select="$VAR-200"/> -->
80
81  <!-- VAR-900 generates the > sign -->
82  <xsl:variable name="VAR-900">&gt;</xsl:variable>
83  <!-- <xsl:copy-of select="$VAR-900"/> -->
84
85  <owl:NamedIndividual>
86  <!-- S10 creation of identity for TwsMo -->
87  <!-- S10.1 identifier for TwsMo from TLSO -->
88  <!-- as can be observed in the line below, everything is on a single line -->
89  <xsl:attribute name="rdf:about">http://www.marcsel.eu/onto/te/_ID_<xsl:copy-of select="$VAR-NAME-TLSO"/></xsl:
        attribute>
90  <xsl:comment>TL2RDF_BE_TwsMo_v301_S10_1 NamedIndividual created </xsl:comment>
91  <xsl:text>&#10;</xsl:text>
92
93  <!-- S10.2 cast into type ID and allocate UUID -->
94  <rdf:type rdf:resource="http://www.marcsel.eu/onto/te/ID"/>
95  <!-- <te:uniqueText rdf:datatype="http://www.w3.org/2001/XMLSchema#string">UUID_Endorser_FOD_Eco_FIXED</te:
        uniqueText> -->
96  <te:uniqueText rdf:datatype="http://www.w3.org/2001/XMLSchema#string">UUID_<xsl:copy-of select="$VAR-NAME-TLSO"
        /></te:uniqueText>
97  <xsl:comment>TL2RDF_BE_TwsMo_v301_S10_2 identity created with UUID </xsl:comment>
98  <xsl:text>&#10;</xsl:text>
99
100 <!-- S10.3 add wasDerivedFrom -->
101 <!-- Name of data source is hardcoded -->
102 <prov:wasDerivedFrom rdf:resource="https://tsl.belgium.be/tsl-be.xml"/>
103 <xsl:comment>TL2RDF_DataSource_TL_v301_S10_3 wasDerivedFrom </xsl:comment>
104 <xsl:text>&#10;</xsl:text>
105
106 <!-- S10.4 add wasAttributedTo agent -->
107 <xsl:copy-of select="$VAR-100"/>prov:wasAttributedTo rdf:resource="http://www.marcsel.eu/onto/te/_<xsl:value-of_
```

```
        select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
<xsl:comment>TL2RDF_DataSource_TL_v301_S10_4 wasAttributedTo TLSO </xsl:comment>
<xsl:text>&#10;</xsl:text>

<!-- S10.5 add wasGeneratedBy activity -->
<prov:wasGeneratedBy rdf:resource="TL2RDF_BE_TwsMo_v301.xsl_execution_2020-12-23"/>
<xsl:comment>TL2RDF_DataSource_TL_v301_S10_5 wasGeneratedBy</xsl:comment>
<xsl:text>&#10;</xsl:text>

</owl:NamedIndividual>


<owl:NamedIndividual>
<!-- S11 creation of identity for identity attestation -->
<!-- S11.1 give name -->
<xsl:attribute name="rdf:about">http://www.marcsel.eu/onto/te/_ID_IdentityAttestation_<xsl:value-of select="$VAR-
      NAME-TLSO"/></xsl:attribute>
<xsl:comment>TL2RDF_BE_TwsMo_v301_S11_1 NamedIndividual created </xsl:comment>
<xsl:text>&#10;</xsl:text>

<!-- S11.2 cast into type ID and allocate UUID -->
<rdf:type rdf:resource="http://www.marcsel.eu/onto/te/ID"/>
<!-- <te:uniqueText rdf:datatype="http://www.w3.org/2001/XMLSchema#string">UUID_ID_IdentityAttestation_FOD_Eco</te
      :uniqueText>-->
<te:uniqueText rdf:datatype="http://www.w3.org/2001/XMLSchema#string">UUID_ID_IdentityAttestation_<xsl:value-of
      select="$VAR-NAME-TLSO"/></te:uniqueText>
<xsl:comment>TL2RDF_BE_TwsMo_v301_S11_2 identity created with UUID</xsl:comment>
<xsl:text>&#10;</xsl:text>

<!-- S11.3 add wasDerivedFrom -->
<!-- Name of data source is hardcoded -->
<prov:wasDerivedFrom rdf:resource="https://tsl.belgium.be/tsl-be.xml"/>
<xsl:comment>TL2RDF_DataSource_TL_v301_S11_3 wasDerivedFrom </xsl:comment>
<xsl:text>&#10;</xsl:text>

<!-- S11.4 add wasAttributedTo agent -->
<xsl:copy-of select="$VAR-100"/>prov:wasAttributedTo rdf:resource="http://www.marcsel.eu/onto/te/_<xsl:value-of_
      select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
<xsl:comment>TL2RDF_DataSource_TL_v301_S11_4 wasAttributedTo TLSO </xsl:comment>
<xsl:text>&#10;</xsl:text>

<!-- S11.5 add wasGeneratedBy activity -->
<prov:wasGeneratedBy rdf:resource="TL2RDF_BE_TwsMo_v301.xsl_execution_2020-12-23"/>
<xsl:comment>TL2RDF_DataSource_TL_v301_S11_5 wasGeneratedBy</xsl:comment>
<xsl:text>&#10;</xsl:text>

</owl:NamedIndividual>


<owl:NamedIndividual>

<!-- S12 creation of identity for role attestation as TwsMo -->
<!-- S12.1 give name -->
<xsl:attribute name="rdf:about">http://www.marcsel.eu/onto/te/_ID_RoleAttestation_TwsMo_<xsl:value-of select="$VAR
      -NAME-TLSO"/></xsl:attribute>
<xsl:comment>TL2RDF_BE_TwsMo_v301_S12_1 NamedIndividual created </xsl:comment>
<xsl:text>&#10;</xsl:text>

<!-- S12.2 cast into type ID and allocate UUID -->
<rdf:type rdf:resource="http://www.marcsel.eu/onto/te/ID"/>
<te:uniqueText rdf:datatype="http://www.w3.org/2001/XMLSchema#string">UUID_ID_RoleAttestation_TwsMo_<xsl:value-of
      select="$VAR-NAME-TLSO"/></te:uniqueText>
<xsl:comment>TL2RDF_BE_TwsMo_v301_S12_2 identity created with UUID</xsl:comment>
<xsl:text>&#10;</xsl:text>

<!-- S12.3 add wasDerivedFrom -->
<!-- Name of data source is hardcoded -->
<prov:wasDerivedFrom rdf:resource="https://tsl.belgium.be/tsl-be.xml"/>
<xsl:comment>TL2RDF_DataSource_TL_v301_S10_3 wasDerivedFrom </xsl:comment>
<xsl:text>&#10;</xsl:text>

<!-- S12.4 add wasAttributedTo agent -->
```

```
173 <xsl:copy-of select="$VAR-100"/>prov:wasAttributedTo rdf:resource="http://www.marcsel.eu/onto/te/_<xsl:value-of_
        select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
174 <xsl:comment>TL2RDF_DataSource_TL_v301_S10_4 wasAttributedTo TLSO </xsl:comment>
175 <xsl:text>&#10;</xsl:text>
176
177 <!-- S12.5 add wasGeneratedBy activity -->
178 <prov:wasGeneratedBy rdf:resource="TL2RDF_BE_TwsMo_v301.xsl_execution_2020-12-23"/>
179 <xsl:comment>TL2RDF_DataSource_TL_v301_S10_5 wasGeneratedBy</xsl:comment>
180 <xsl:text>&#10;</xsl:text>
181
182 </owl:NamedIndividual>
183
184
185 <owl:NamedIndividual>
186 <!-- S20 creation of identity attestation -->
187 <!-- create individual of type te:IdentityAttestation, relate it to its identity -->
188 <!-- S20.1 give name -->
189 <!-- e.g. _IdentityAttestation_Certipost%20n.v./s.a. -->
190 <xsl:attribute name="rdf:about">http://www.marcsel.eu/onto/te/_IdentityAttestation_<xsl:value-of select="$VAR-NAME
        -TLSO"/></xsl:attribute>
191 <xsl:comment>TL2RDF_BE_TwsMo_v301_S20_1 NamedIndividual created </xsl:comment>
192 <xsl:text>&#10;</xsl:text>
193
194 <!-- S20.2 cast into type IdentityAttestation -->
195 <rdf:type rdf:resource="http://www.marcsel.eu/onto/te/IdentityAttestation"/>
196 <xsl:comment>TL2RDF_BE_TwsMo_v301_S20_2 casted into type IdentityAttestation</xsl:comment>
197 <xsl:text>&#10;</xsl:text>
198 <xsl:copy-of select="$VAR-100"/>te:identifiedBy rdf:resource="http://www.marcsel.eu/onto/te/
        _ID_IdentityAttestation_<xsl:value-of_select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
199
200 <!-- S20.3 comment -->
201 <xsl:text>&#10;</xsl:text>
202 <xsl:comment>TL2RDF_BE_TwsMo_v301_S20_3 _IdentityAttestation identifiedBy _ID_IdentityAttestation_ </xsl:comment>

203 <xsl:text>&#10;</xsl:text>
204
205 <!-- S20.4 relate to IdentityAttestation -->
206 <xsl:copy-of select="$VAR-100"/>te:identityAttestationID rdf:resource="http://www.marcsel.eu/onto/te/_ID_<xsl:
        value-of_select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
207 <xsl:comment>TL2RDF_BE_TwsMo_v301_S20_4 identity attestation via identityAttestationID related to _ID_ </xsl:
        comment>
208 <xsl:text>&#10;</xsl:text>
209
210 <!-- S20.5 add wasDerivedFrom -->
211 <!-- Name of data source is hardcoded -->
212 <prov:wasDerivedFrom rdf:resource="https://tsl.belgium.be/tsl-be.xml"/>
213 <xsl:comment>TL2RDF_DataSource_TL_v301_S20_5 wasDerivedFrom </xsl:comment>
214 <xsl:text>&#10;</xsl:text>
215
216 <!-- S20.6 add wasAttributedTo agent -->
217 <xsl:copy-of select="$VAR-100"/>prov:wasAttributedTo rdf:resource="http://www.marcsel.eu/onto/te/_<xsl:value-of_
        select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
218 <xsl:comment>TL2RDF_DataSource_TL_v301_S20_6 wasAttributedTo TLSO </xsl:comment>
219 <xsl:text>&#10;</xsl:text>
220
221 <!-- S20.7 add wasGeneratedBy activity -->
222 <prov:wasGeneratedBy rdf:resource="TL2RDF_BE_TwsMo_v301.xsl_execution_2020-12-23"/>
223 <xsl:comment>TL2RDF_DataSource_TL_v301_S20_7 wasGeneratedBy</xsl:comment>
224 <xsl:text>&#10;</xsl:text>
225
226 </owl:NamedIndividual>
227
228
229 <owl:NamedIndividual>
230 <!-- S21 role attestation TwsMo -->
231 <!-- create individual of type te:RoleAttestation, relate it to its identity -->
232 <!-- S21.1 give name -->
233 <!-- e.g. _RoleAttestation_Certipost%20n.v./s.a. -->
234 <xsl:attribute name="rdf:about">http://www.marcsel.eu/onto/te/_RoleAttestation_TwsMo_<xsl:value-of select="$VAR-
        NAME-TLSO"/></xsl:attribute>
235 <xsl:comment>TL2RDF_BE_TwsMo_v301_S21_1 NamedIndividual created </xsl:comment>
236 <xsl:text>&#10;</xsl:text>
```

```
237
238 <!-- S21.2 cast into type RoleAttestation -->
239 <rdf:type rdf:resource="http://www.marcsel.eu/onto/te/RoleAttestation"/>
240 <xsl:comment>TL2RDF_BE_TwsMo_v301_S21_2 casted to type RoleAttestation</xsl:comment>
241 <xsl:text>&#10;</xsl:text>
242
243 <!-- S21.3 identified by -->
244 <xsl:copy-of select="$VAR-100"/>te:identifiedBy rdf:resource="http://www.marcsel.eu/onto/te/
       _ID_RoleAttestation_TwsMo_<xsl:value-of_select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
245 <xsl:text>&#10;</xsl:text>
246 <xsl:comment>TL2RDF_BE_TwsMo_v301_S21_3 _RoleAttestation identifiedBy _ID_RoleAttestation_ </xsl:comment>
247 <xsl:text>&#10;</xsl:text>
248
249 <!-- S21.4 relate attestation individual to TwsMo role -->
250 <te:roleAttestationR rdf:resource="http://www.marcsel.eu/onto/te/_TwsMo"/>
251 <xsl:comment>TL2RDF_BE_TwsMo_v301_S21_4 role attestation related to _TwsMo role </xsl:comment>
252 <xsl:text>&#10;</xsl:text>
253
254 <!-- S21.5 add wasDerivedFrom -->
255 <!-- Name of data source is hardcoded -->
256 <prov:wasDerivedFrom rdf:resource="https://tsl.belgium.be/tsl-be.xml"/>
257 <xsl:comment>TL2RDF_DataSource_TL_v301_S21_5 wasDerivedFrom </xsl:comment>
258 <xsl:text>&#10;</xsl:text>
259
260 <!-- S21.6 add wasAttributedTo agent -->
261 <xsl:copy-of select="$VAR-100"/>prov:wasAttributedTo rdf:resource="http://www.marcsel.eu/onto/te/_<xsl:value-of_
       select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
262 <xsl:comment>TL2RDF_DataSource_TL_v301_S21_6 wasAttributedTo TLSO </xsl:comment>
263 <xsl:text>&#10;</xsl:text>
264
265 <!-- S21.7 add wasGeneratedBy activity -->
266 <prov:wasGeneratedBy rdf:resource="TL2RDF_BE_TwsMo_v301.xsl_execution_2020-12-23"/>
267 <xsl:comment>TL2RDF_DataSource_TL_v301_S21_7 wasGeneratedBy</xsl:comment>
268 <xsl:text>&#10;</xsl:text>
269
270 </owl:NamedIndividual>
271
272
273 <owl:NamedIndividual>
274 <!-- S30 creation of TwsMo -->
275 <!-- S30.1 give name -->
276 <xsl:attribute name="rdf:about">http://www.marcsel.eu/onto/te/_<xsl:value-of select="$VAR-NAME-TLSO"/></xsl:
       attribute>
277 <xsl:text>&#10;</xsl:text>
278 <xsl:comment>TL2RDF_BE_TwsMo_v301_S30_1 NamedIndividual created</xsl:comment>
279 <xsl:text>&#10;</xsl:text>
280
281 <!-- S30.2 relate to its own identity -->
282 <xsl:copy-of select="$VAR-100"/>te:identifiedBy rdf:resource="http://www.marcsel.eu/onto/te/_ID_<xsl:value-of_
       select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
283 <xsl:comment>TL2RDF_BE_TwsMo_v301_S30_2 NamedIndividual identifiedBy _ID_ </xsl:comment>
284 <xsl:text>&#10;</xsl:text>
285
286 <!-- S30.3 cast into type of org organisation -->
287 <rdf:type rdf:resource="http://www.w3.org/ns/org#Organization"/>
288 <xsl:comment>TL2RDF_BE_TwsMo_v301_S30_3 NamedIndividual cast into type org:Organization </xsl:comment>
289 <xsl:text>&#10;</xsl:text>
290
291 <!-- S30.4 cast into type of prov organisation -->
292 <rdf:type rdf:resource="http://www.w3.org/ns/prov#Organization"/>
293 <xsl:comment>TL2RDF_BE_TwsMo_v301_S30_4 NamedIndividual cast into type prov:Organization </xsl:comment>
294 <xsl:text>&#10;</xsl:text>
295
296 <!-- S30.5 self attest identity -->
297 <xsl:copy-of select="$VAR-100"/>te:pIdentityAttestation rdf:resource="http://www.marcsel.eu/onto/te/
       _IdentityAttestation_<xsl:value-of_select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
298 <xsl:comment>TL2RDF_BE_TwsMo_v301_S30_5 NamedIndividual identity self-attestation </xsl:comment>
299 <xsl:text>&#10;</xsl:text>
300
301 <!-- S30.6 self attest TwsMo role -->
302 <xsl:copy-of select="$VAR-100"/>te:pRoleAttestation rdf:resource="http://www.marcsel.eu/onto/te/
       _RoleAttestation_TwsMo_<xsl:value-of_select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
```

```
303 <xsl:comment>TL2RDF_BE_TwsMo_v301_S30_6 NamedIndividual role self-attestation as TwsMo </xsl:comment>
304 <xsl:text>&#10;</xsl:text>
305
306 <!-- S30.7 add wasDerivedFrom -->
307 <!-- Name of data source is hardcoded -->
308 <prov:wasDerivedFrom rdf:resource="https://tsl.belgium.be/tsl-be.xml"/>
309 <xsl:comment>TL2RDF_DataSource_TL_v301_S30_7 wasDerivedFrom </xsl:comment>
310 <xsl:text>&#10;</xsl:text>
311
312 <!-- S30.8 add wasAttributedTo agent -->
313 <xsl:copy-of select="$VAR-100"/>prov:wasAttributedTo rdf:resource="http://www.marcsel.eu/onto/te/_<xsl:value-of_
        select="$VAR-NAME-TLSO"/>"/<xsl:copy-of select="$VAR-900"/>
314 <xsl:comment>TL2RDF_DataSource_TL_v301_S30_8 wasAttributedTo TLSO </xsl:comment>
315 <xsl:text>&#10;</xsl:text>
316
317 <!-- S30.9 add wasGeneratedBy activity -->
318 <prov:wasGeneratedBy rdf:resource="TL2RDF_BE_TwsMo_v301.xsl_execution_2020-12-23"/>
319 <xsl:comment>TL2RDF_DataSource_TL_v301_S30_9 wasGeneratedBy</xsl:comment>
320 <xsl:text>&#10;</xsl:text>
321
322 </owl:NamedIndividual>
323
324 </xsl:template>
325
326 <xsl:template match="/">
327 <xsl:text>&#10;</xsl:text>
328 <rdf:RDF>
329 <xsl:text>&#10;</xsl:text>
330 <xsl:apply-templates select="/tsl:TrustServiceStatusList/tsl:SchemeInformation/tsl:SchemeOperatorName"/>
331 <xsl:text>&#10;</xsl:text>
332 </rdf:RDF>
333 <xsl:text>&#10;</xsl:text>
334 </xsl:template>
335
336 </xsl:stylesheet>
```

Appendix L

Data integration

This appendix describes how the output files of the transformations were combined into a single file that can be used to load into an OWL-capable tool such as a graph database.

L.1 Construction of the database load file

The outputs of all transformations were included in a single XML/RDF file. This integrated file is referred to as the database load file. Its filename is *DBL.owl*.

The database load file *DBL.owl* was constructed as follows.

- The data model was inserted from the `http://www.marcsel.eu/onto/te/te-data-model.owl` file.
- The legal norms and standards were inserted from the *DBLN.owl* file.
- The self-attestations were inserted from the *DBLS.owl* file.
- The output files of the transformations were added, as well as the manually created rdf files in case no transformation was involved (e.g. in the case of the manual creation of a data source assertion).
- Interim files were used to aggregate data as described below.

L.2 DBL1 Trusted List data

Aggregation of TL data (*DBL1.owl*):

- The following data sources were combined into *DBL.1.DataSources.rdf*:

  - *TL2RDF_BE_DataSource_TL_v301.rdf*,
  - *TL2RDF_ES_DataSource_TL_v301.rdf*,
  - *TL2RDF_UK_DataSource_TL_v301.rdf*.

- The following trustworthiness monitors were combined into *DBL.1.TwsMos.rdf*:

  - *TL2RDF_BE_TwsMo_v301.rdf*,
  - *TL2RDF_ES_TwsMo_v301.rdf*,
  - *TL2RDF_UK_TwsMo_v301.rdf*.

- The following evidence service providers were combined into *DBL.1.EvSPs.rdf*:

  - *TL2RDF_BE_EvSPs_v301.rdf*,
  - *TL2RDF_ES_EvSPs_v301.rdf*,
  - *TL2RDF_UK_EvSPs_v301.rdf*,
  - *PDF2RDF-UK-EvSP-tScheme-v301.rdf*.

  The first three files were based on LOTL transformations, and the fourth file was based on a review of the information published by tScheme.

L.3 DBL2 List of Trusted Lists data

Aggregation of LOTL data (*DBL2.owl*):

- Data source: *TL2RDF_DataSource_LOTL_v301.rdf*,
- EC as trustworthiness monitor: *TL2RDF_LOTL_1_v301.rdf*,
- identity and role attestations for trustworthiness monitors: *TL2RDF_LOTL_2_v301.rdf*,

L.4 DBL3 accreditation data

The following files were combined in *DBL3.rdf*:

- *DBL3.DataSource.owl*, which contains:

  - *PDF2RDF_DataSource_BELAC_v301.rdf*,
  - *PDF2RDF_DataSource_COFRAC_v301.rdf*,

  - *PDF2RDF_DataSource_EA_v301.rdf*,
  - *PDF2RDF_DataSource_ENAC_v301.rdf*,
  - *PDF2RDF_DataSource_UKAS_v301.rdf*.

- *DBL3.AB.owl*, which contains:
  - *PDF2RDF_BE_BELAC_v301.rdf*,
  - *PDF2RDF_FR_COFRAC_v301.rdf*,
  - *PDF2RDF_UK_UKAS_v301.rdf*.

- *DBL3.CAB.owl*, which contains:
  - *PDF2RDF_BE_BELAC_CABs_v301.rdf*,
  - *PDF2RDF_FR_COFRAC_CABs_v301.rdf*,
  - *PDF2RDF_UK_UKAS_CABs_v301.rdf*.

- *DBL3.EvSP.owl*, which contains:
  - *PDF2RDF_FR_LSTI_EvSPs_v301.rdf*.

L.5 DBL4 company data

Aggregation of company data (*DBL.4.rdf*), which contains:

- Data source *FF-DataSource-v301.rdf*,
- Legal persons *FFLEI2RDF_v301.extract.rdf*.

L.6 DBL5 natural persons data

Aggregation of natural person data (*DBL.5.rdf*) was done as follows.

- The following data sources were combined into *DBL.5.DataSources.rdf*:
  - *FOAF_01_DataSource_v301.rdf*,
  - *FOAF_02_DataSource_v301.rdf*,
  - *Certipost-CitizenCA_01_DataSource_v301.rdf*.

- The following natural persons files were combined into *DBL.5.NPs.rdf*:

- *FOAF_01_NP_v301.rdf*,
- *FOAF_02_NP_v301.rdf*,
- *Certipost-CitizenCA_01_NP_v301.rdf*.

L.7 DBL6 authentic sources

The *DBL6.AS.owl* file was integrated. It contained a copy of the file *BE-AS-NRN-v301.rdf*.

L.8 DBL7 rulebook

The *DBL7.Rulebook.owl* file, containing individuals that represent rulebooks[1], was integrated.

[1] A copy of the content of the rulebook developed during the implementation is available from `http://www.marcsel.eu/onto/te/Rulebook.txt`

Appendix M

Additional SPARQL code

This appendix contains additional SPARQL code. It demonstrates how SPARQL queries can be used to query the graph that was created as part of the implementation of the $\mathcal{TE}$ framework.

M.1 Additional SPARQL

M.1.1 IR3-M01-EvSP

IR3-M01-EvSP is a refinement of IR3-M01. The refinement is described in Listing M.1. It adds the condition that the participant must be an EvSP to IR3-M01. The expected result is that the potential trustee is included in the list.

Listing M.1: IR3-M01-EvSP

```
\# IR3-M01-EvSP
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
select DISTINCT ?Participant ?Role where {
    ?Participant rdf:type te:Participant .
        ?identifier te:doesIdentify ?Participant .
    ?Participant te:pIdentityAttestation ?IdentityAttestationOfParticipant .
    ?Participant te:pRoleAttestation ?RoleAttestationOfParticipant .
    ?RoleAttestationOfParticipant te:roleAttestationR te:EvSP .
    ?RoleAttestationOfParticipant te:roleAttestationR ?Role .
}
```

M.1.2 IRX-Legal-Attestations

Listing M.2 implements the query whose result lists all participants for which a legal attestation was created on the basis of a legal document.

Listing M.2: IRX-Legal-Attestations

```
# IRX-Legal-Attestations
# List all participants legally attested in their role
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
?P1 te:pRoleAttestation ?RoleAttestationOfP1 .
?RoleAttestationOfP1 te:raLegalQualification ?LegalRoleQualification .
?LegalRoleQualification te:legalQualificationN ?LegalNorm.
}
```

M.1.3 IRX-Sources-of-Role-Attestations

Listing M.3 implements the query whose result lists a selection of the sources where role attestations were derived from.

Listing M.3: IRX-Sources-of-Role-Attestations

```
# IRX-Sources-of-role-attestations for EvSPs
# Lists all evidence service providers and where their role attestations were derived from
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
?EvSP te:pRoleAttestation ?RoleAttestation .
?RoleAttestation te:roleAttestationR te:EvSP .
?RoleAttestation prov:wasDerivedFrom ?wasDerivedFrom .
}
```

M.1.4 IRX-Participants-conformance

Listing M.4 implements the query whose result lists all participants and the standards they have a conformance attestation for.

Listing M.4: IRX-Participants-conformance

```
# IRX-Participants-conformance
# List all participants with conformance attestations
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX te: <http://www.marcsel.eu/onto/te/>
PREFIX prov: <http://www.w3.org/ns/prov#>
select * where {
?P1 te:pConformance ?ConformanceAttestationOfP1 .
?ConformanceAttestationOfP1 te:conformanceN ?Standard .
}
```

Appendix N

Selected rules of rulebook β_{AE}

This appendix describes an implementation of the discretionary rules for requirement IR2 for the rulebook β_{AE}.

For rulebook β_{AE}, the discretionary rules regarding transparency were specified in Tables 8.1, 8.2 and 8.3. The rules contained in Table 8.1 (the enabler-plane rules) were implemented in the following way.

- Rules $\beta_{IR2\text{-}D01A\text{-}AE}$ (a trustworthy ecosystem must contain at least one endorser) and $\beta_{IR2\text{-}D01B\text{-}AE}$ (a trustworthy ecosystem must contain at least one enforcer) were implemented together as described in Listing N.1. The expected response is YES.

- Rule $\beta_{IR2\text{-}D02\text{-}AE}$ (a trustworthy ecosystem must contain at least one authentic source), $\beta_{IR2\text{-}D03\text{-}AE}$ (a trustworthy ecosystem must contain at least one accreditation body) and $\beta_{IR2\text{-}D04\text{-}AE}$ (a trustworthy ecosystem must contain at least one conformity assessment body) were implemented together as described in Listing N.2. The expected response is YES.

The rules contained in Table 8.2 (the trustworthiness provision plan rules) were implemented by combining the three rules: $\beta_{IR2\text{-}D05\text{-}AE}$ (a trustworthy ecosystem must contain at least one evidence service provider), $\beta_{IR2\text{-}D06\text{-}AE}$ (a trustworthy ecosystem must contain at least one claim status service provider) and $\beta_{IR2\text{-}D07\text{-}AE}$ (a trustworthy ecosystem must contain at least one trustworthiness monitor), as described in Listing N.3. The expected response is YES.

The rules contained in Table 8.3 (the functional plane rules) were implemented by combining the two rules: $\beta_{IR2\text{-}D08\text{-}AE}$ (a trustworthy ecosystem must contain at least one functional service provider) and $\beta_{IR2\text{-}D09\text{-}AE}$ (a trustworthy ecosystem must contain at least one functional service consumer), as described in Listing N.4. The expected response is YES.

Listing N.1: IR2-D01A-AE and -D01B-AE

```
# IR2-D01A-AE and -D01B-AE
ASK {
?p1 te:pRoleAttestation ?roleatt .
 ?roleatt te:roleAttestationR te:EnDo .
?p2 te:pRoleAttestation ?roleatt2 .
?roleatt2 te:roleAttestationR te:EnFo .
}
```

Listing N.2: IR2-D02-AE -D03-AE -D04-AE

```
# IR2-D02-AE -D03-AE -D04-AE
ASK {
?p3 te:pRoleAttestation ?roleatt3 .
?roleatt3 te:roleAttestationR te:AS .
?p4 te:pRoleAttestation ?roleatt4 .
?roleatt3 te:roleAttestationR te:AB .
?p5 te:pRoleAttestation ?roleatt5 .
?roleatt5 te:roleAttestationR te:CAB .
}
```

Listing N.3: IR2-D05-AE -D07-AE

```
# IR2-D05-AE -D07-AE
ASK {
?p5 te:pRoleAttestation ?roleatt5 .
?roleatt5 te:roleAttestationR te:EvSP .
?p6 te:pRoleAttestation ?roleatt6 .
?roleatt6 te:roleAttestationR te:CsSP .
?p7 te:pRoleAttestation ?roleatt7 .
?roleatt7 te:roleAttestationR te:TwSMo .
}
```

Listing N.4: IR2-D08-AE -D09-AE

```
# IR2-D08-AE -D09-AE
ASK {
?p8 te:pRoleAttestation ?roleatt8 .
?roleatt8 te:roleAttestationR te:FuSP .
?p9 te:pRoleAttestation ?roleatt9 .
?roleatt9 te:roleAttestationR te:FuSC .
}
```