Application Management Framework in User Centric Smart Card Ownership Model

Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes

Information Security Group Smart card Centre, Royal Holloway, University of London
Egham, Surrey, United Kingdom
{R.N.Akram, K.Markantonakis, Keith.Mayes}@rhul.ac.uk

Abstract. The predominant smart card ownership model is the issuer centric, and it has played a vital role in the proliferation of the technology. However, recent developments of multi-application smart card technology lead to new potential ownership models. One of the possible models is the User Centric Smart Card Ownership Model. In this model, the ownership is with smart card users. To support user's ownership, we require a framework that can assist cardholders to manage applications on their smart cards. In this paper, we present such a framework for managing application securely on a smart card.

1 Introduction

Historically, the smart card ownership resides with organizations (card issuers) that provide smart card based services. Smart cards issued by the card issuer will have pre-installed applications, and they cannot customise to suit customer's requirements. This ownership model lacks flexibility, ubiquity and is inconvenient to cardholders.

In last two decades, the smart card technology evolved to support multiple applications. The adoption of multi-application smart cards was hindered by card issuers concerns over the ownership of the card and customer relationship along with branding issues. A possible solution to these issues is to delegate the ownership to users. This proposal is referred to as the User Centric Smart Card Ownership Model (UCOM), which is based on providing the complete control over the choice of applications on a smart card, securely and efficiently, to its cardholder. To do so, cardholders would require a secure and practical mechanism to perform application management tasks efficiently. In this paper, we discuss the need for the new ownership model and describe how it is different from the existing models. The main focus of the paper is the procedures and functions performed by a smart card and a service provider to install or delete an application in the UCOM.

In section two, a short description of the UCOM is provided along with the motivation for the new ownership model. Section three describes the architecture of the Application Management Framework (AMF) that supports the application installation and deletion process on the UCOM-based smart cards. The

application management processes (e.g. install, delete, etc) are described in section four. Section five provides an analysis of the proposed framework. Section six briefly looks on future research directions and finally, section seven draws the conclusion.

2 User Centric Smart Card Ownership Model

In the following sections we provide the motivation behind the User Centric Smart Card Ownership Model (UCOM) proposal along with its architectural overview.

2.1 Motivation

The multi-application smart card technology, except for the initial popularity it never took off. However, recent developments mainly driven by the technologies like Near Field Communication (NFC) [**?**] and Secure Element (SE) [2] in mobile phones have revived again the concept of having multi-applications on a smart card (chip).

The NFC enables a contactless data exchange between a chip (i.e. smart card) and the terminal. It is also extended to include the mobile phones that enable them to emulate the contactless smart cards. As a result, the existing infrastructure deployed in the different industries (i.e. banking, transport, access control) to support contactless smart card can be utilised. There are many organisations around the world that are currently engaged in the field trials [3, 4, 5], and they are fostering new business models to actively manage the multi-applications through mobile phones.

To support the initiative, there are many different proposals to manage the SE in the NFC based mobile phones. One proposal is to keep the traditional ownership model so that the card issuer (i.e. Telecom) will have the ownership. This model has traditional issues related to the ownership of smart cards and customer relationship. Another model is to delegate the control to a third party that does not use the SE to provide any services to end users. Such a model is referred to as the "Trusted Service Manager" (TSM) based model [6]. In this model, the trust relationships with Telco operators and other service providers are maintained by the TSMs. Eventually it enables the SE to host multiple applications from different companies). Each company only has to establish an individual trust relationship with a TSM.

However, the UCOM goes further by giving choice of applications on a card to its user. The card assures a Service Provider (SP) of its underlying security state and if satisfied the SP's is satisfied; it can lease its application(s). The difference between the TSM and UCOM is that TSM still requires trust relationship between service providers and a TSM that may involve business and financial agreements. This may discourage small businesses (e.g. public library, health centre, leisure club). In the UCOM the small companies only require to

develop their applications, and they can be installed onto their customer's SE in a cost effective way.

The multi-application smart cards platforms (i.e. Java [7], Multos [8]) support the installation of applications remotely (after issuance of the card). The standardisation efforts to manage the application remotely like the GlobalPlatform [9] have been effective in the Issuer Centric Smart Card Ownership Model (ICOM). In the ICOM, the control of the card is with a single organisation and they manage the relationship with other organisations that may wish to share the smart card. In these situations, there is always an entity (i.e. card issuer) that has a pre-issuance secure binding with the smart card. The security measures are implemented by card issuers and they provide the security assurance. The pre-issuance secure binding and control of security measures implemented on smart cards provides a secure and reliable model. This notion is based on the presumption that the ICOM is a closed environment and applications are rarely installed and deleted from a card.

The ICOM based frameworks including the GlobalPlatform are proposed with the assumption that the ownership will be either with a card issuer or a third party. This assumption is not necessarily constructive when dealing with the user's ownership of the smart card. The ownership gives the provision to install and delete any application that also brings new security and privacy issues that are not present in the ICOM. The presented proposal is designed with a basic principle that the underlying platform is open, dynamic and in the control of its user that may act as adversary.

2.2 Overview of the User Centric Smart Card Ownership Model

The User Centric Smart Card Ownership Model (UCOM) focuses on the delegation of the ownership (control) to its users. The term "Ownership" in the UCOM does not imply that users own the application(s) installed onto their smart card(s). It only means the freedom of choice to install or delete any application(s). The ownership of applications will always remain with their corresponding SP. The SPs will only lease their applications, after specific security, privacy and operational requirements are satisfied by the UCOM-based smart card. The provision to install or delete an application cannot be performed without the prior authorisation of the relevant SP.

The UCOM-based smart cards should support the ownership of the cardholder and provide adequate functionality for the application management tasks. In addition, it should provide security assurances to SPs who lease their applications. As a crucial design requirement a UCOM-based smart card should be an impartial, secure and robust platform. The impartiality in the UCOM refers to providing assurance that the card does not favour any application or particular set of applications. The following figure illustrates the architectural overview of the UCOM.

In the UCOM, a cardholder acquires a smart card from UCSC supplier. A smart card that supports UCOM is referred to as User Centric Smart Card (UCSC) and a UCSC supplier can be a smart card manufacturer, an SP or a

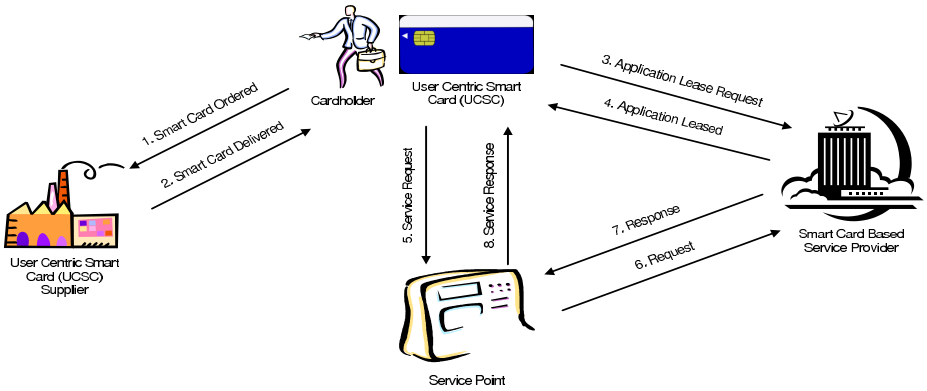

Fig. 1. Illustration of the User Centric Smart Card Ownership Model (UCOM)

third party vendor. After acquiring the UCSC, the cardholder can request an SP to lease its application(s). The SP will decide the lease based on its Application Lease Policy (ALP). If the requesting UCSC meets the ALP, the application is leased, otherwise the request is denied. In addition to requesting the lease of an application, the cardholder could also request the removal.

An Application Lease Policy (ALP) defines the minimum requirement of an SP that an UCSC has to satisfy. The APL not only governs the lease of the application(s), but also the terms of the lease. The terms of the lease stipulate the minimum security, privacy and operational requirements of an application while it is installed onto an UCSC. The UCSC will provide adequate measures to enable an application to verify the execution environment before executing. Furthermore, the lease of an application can be temporary (time/execution constraint) as defined by the ALP. The UCSC or the application will initiate the deletion command once it reaches the expiry. After application(s) is leased, the cardholder can request the SP's associated services that are entitled to the cardholder (application) via a service point. A service point is a point of service device (i.e. ATM, Access Controllers) where a user presents his/her smart card to utilise certain services. The basic function of a service point is to connect an application to the relevant SP, so the application can authenticate itself before the user is being facilitated by the service point in accessing the SP's services.

SPs will make their application for installation ubiquitously accessible to their customers by offering them through a web server, referred as an Application Management Server (AMS). In addition to the AMS, SPs also have an Application Services Authentication Server (ASAS). These two servers are essential to support the UCOM from SPs perspective. SPs will provide their customers with the AMS credentials (i.e. AMS web address) and user's credentials (i.e. Account ID, login/password) that they can use to access and authenticate to the AMS.

An AMS typically deals with the application management processes (i.e. installation, deletion). The application management processes also include enforcing the ALP, ensuring that the application is transmitted and installed securely

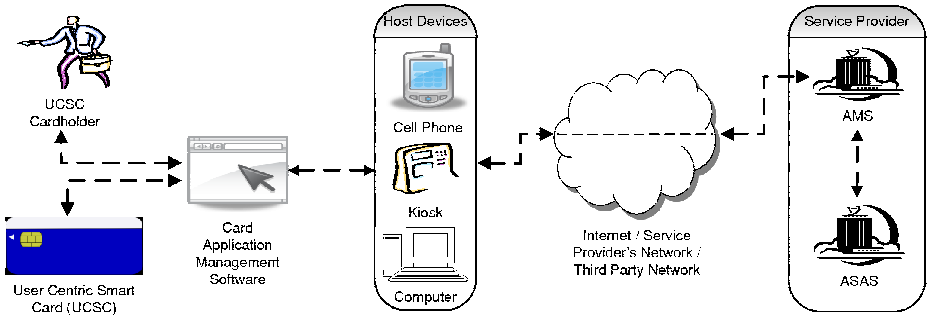

Fig. 2. Illustration of Application Management Framework

onto a smart card, and managing a user's profile. The user's profile keeps record of the registered smart cards and card(s) that hold the active lease. Depending upon an SP's ALP, a user can have the application installed onto multiple cards; therefore, the AMS keeps track of all cards of a particular user that hold/held the lease.

3 Application Management Framework

An overview of the framework is provided in section 3.1. Section 3.2 explains the basic UCSC configuration required to support the framework. The establishment of a secure connection between an UCSC and an SP's AMS is described in section 3.3.

3.1 Application Management Framework Overview

The UCOM Application Management framework (AMF) that stipulates the mechanism of application installation and deletion is illustrated in Figure 2. To initiate the AMF processes a cardholder presents his/her UCSC to a host device. A host device (i.e. cell phones, kiosks, and computers) acts as the connection bridge between the smart card (i.e. UCSC) and the AMS. The cardholder will provide his/her account credentials for an AMS to the Card Application Management Software (CAMS). The basic functionality of the CAMS is to provide an interface (between a cardholder, UCSC and AMS) and protocol conversion (if required). The protocol conversion addresses any incompatibilities between a smart card and an AMS supported protocols. For example, a smart card may not support TCP/IP protocol so protocol conversion will provide the TCP/IP support. After a cardholder's authentication with an AMS, a secure channel is established (section 3.3) between the UCSC and AMS. The next phase involves the initiation of the required tasks (i.e. installation, deletion, etc) that are discussed in section 4.

3.2 Basic User Centric Smart Card Configuration

The basic design principle of the UCOM is to be independent of underlying Smart Card Operating System (SCOS) [10] or platform. However, for practical and security reasons we have to define the minimum requirements for different components of the UCOM. The minimum requirement that a UCSC should satisfy for the AMF is to have an SSL/TLS public key pair and public key certificate [11]. A UCSC will have a SSL/TLS public key pair and certificate, irrespectively of the underlying protocol (i.e. TCP/IP [12] and SSL/TLS [11]) handling. If an UCSC supports a web server [16] along with the TCP/IP and SSL/TLS protocols, the secure communication channel would be established entirely by the UCSC, otherwise the CAMS should provide the protocol conversion functionality. In any situation, all cryptographic functions are only handled by the UCSC.

The AMF uses both symmetric and asymmetric cryptography [13] to provide security and privacy services. The cryptographic keys used beside the SSL/TLS keys are generated by the AMSs and smart cards. These keys are lease specific and when the lease expires or the cardholder requests the deletion of the application, all cryptographic keys associated with the application will also be deleted. The UCSC supports the domain mechanism for post-installation application lifecycle management as in the GlobalPlatform (GP) [9]. The subtle difference between the GP and UCOM domain mechanism is the non-availability of Issuer's Domain. In addition, no entity (i.e. card manufacturer, SP and cardholder) has ownership of the security domain of the UCSC. The reason for not giving the control of the security domain is to avoid the possibility of indirect control of the UCSC and also to ensure SPs that there will not be any over-riding privileges for an entity.

The UCSCs will have adequate mechanisms to ensure SPs that they satisfy their ALP. One of the integral parts of the ALP requirement verification is the validation of the security of an UCSC. The existing security validation is based on initiating the security evaluation of the smart card according to the Common Criteria (CC) [14]. At the end of the Common Criteria Evaluation, the smart card is given the Common Criteria Security Evaluation Assurance Level (EAL). The EAL determines how thoroughly the evaluation is performed and the security of the underlying hardware and software. In the ICOM environment, the EAL is not present on the smart card and it is a certificate that is mostly kept off-card by the organisation (card issuers). However, in the UCOM the Common Criteria Security EAL can play an important role to certify the level of security assurance that an UCSC provides. This can be done by the on-card Common Criteria Security Evaluation Certificate (CC-Certificate). The certificate is cryptographically protected in order to provide the EAL of the platform. As the certificate can only provide assurance of the state of the security at the time of evaluation and the card manufacture may opt to deploy weaker security. To avoid this, the certificate also contains an image (created by cryptographic hash function [13]) of the underlying hardware and software. The smart card itself or an SP's application can request the self-test of the card to

gain the assurance of the security. The self-test basically generates the image of the underlying software (Smart Card Operating System) and optional hardware configurations. This image is then verified with the image associated with CC-Certificate. If both match, it can be safe to assume that the platform is at similar state as it was when the CC evaluation was carried out. To perform the image measurement and then comparison, the possible solution can be a Trusted Platform Module (TPM) [15] for the smart card. The scope of exact solution to provide the assurance for the security of an UCSC and how different components will interact with each other is beyond the scope of this paper.

3.3 Secure Channel Establishment between an UCSC and an AMS

A cardholder will initiate the connection with an AMS through the CAMS interface. The user provides the AMS details (e.g. web address) to the CAMS. that initiates a connection. The AMS establishes a secure connection (i.e. SSL/TLS [12]) with the requesting CAMS. After establishing the connection, the AMS requests the user's credentials. The user provides his/her credentials (i.e. account ID, login/password) through the CAMS interface. The details and type of the credentials are on the SP's sole discretion. The AMS verifies the credentials, if it is successful, it will allow the access to its services, and otherwise the connection is terminated. After the authentication the two-way SSL/TLS [12] session is established between the smart card and the AMS. There are well tested and secure protocols already in the public domain; therefore, this paper does not focus on designing a new protocol. However, the secure channel protocol established between the smart card and the AMS should be based on Public Key cryptosystem (e.g. SSL/TLS). After a secure channel protocol between a smart card and an AMS is established then cardholders can request application installation or deletion, which will be discussed in the next section.

4 Application Management Processes

In this section the crucial process of installation of an application is described in section 4.1.

4.1 Installation Process

In this section, the processes that support the secure transmission and installation of an application are discussed. In the ICOM based environment, there are many secure and robust application delivery mechanisms, most notably by the GlobalPlatform.

Most of these mechanisms rely on the assumption that the smart card is in a closed environment and under the total control of the card issuer. The card issuer has a secure binding with their smart cards before they are issued to their customers. Therefore, there is an implicit trust on the smart card in the ICOM, and most of the protocols are based on it. However in the UCOM, there

is no implicit trust on the smart card. Therefore, the installation process has not only to take this into account but also that the smart card can be under the control of a malicious user, or it may not be a real smart card (card emulator running on a personal computer). The installation process discussed in this section builds the additional checks around the existing application installation protocols (without preferring anyone) that can provide the assurance of secure and reliable application installation.

The installation request will initiate the process of acquiring an application from an AMS and install it on a UCSC. The entire process can be divided into six sub processes listed below.

1. Requirement Verification
2. Domain Creation
3. Downloading
4. Application Verification by card
5. Localisation (Installation)
6. Personalisation
7. Application Registration by AMS

Each of these sub-processes is explained in sections 4.1.1 to 4.1.7. The application deletion process is similar but the steps will be performed in reverse order.

4.1.1 Requirement Verification. Before the lease of an application, the AMS will verify the compliance of an UCSC with its ALP. This verification is illustrated by the flowchart shown in figure 3.

A UCSC creates the Application Request message that contains the UCSC details. The details include the CC-Certificate, UCSC manufacturer certificate, details of the SCOS/runtime environment (i.e. Java Card [7], Multos [8], etc), supported cryptographic algorithms, and communication interfaces (e.g. T1, T2 or CL [10], web [16]]). The manufacturer certificate validates the cryptographic public keys pair and hardware tag. The hardware tag is unique sequence that identifies the UCSC. The length of the tag and how it is generated is on the sole discretion of the UCSC manufacturer. Requirements on the hardware tag by the UCOM are that it does not violate the privacy of the cardholder and actively verifies that the AMS is communicating with the real card (not an emulator).

The AMS will verify whether the requesting UCSC satisfies the ALP. If so, it continues, otherwise process terminates. To verify the CC-Certificate and UCSC manufacturer certificate, the AMS can communicate with either the entity that has issued these certificates, or a third party that plays the role of intermediary between the AMS and the UCSC manufacturers. To validate that the AMS is communicating with a real smart card (not an emulator), the AMS can request the UCSC manufacturer to verify the claim of their card. The details of these processes are beyond the scope of the paper.

After validation of the ALP, the AMS generates application requirement details. This contains the application space and on-card security policy requirements. Application space requirement stipulates the memory required for the

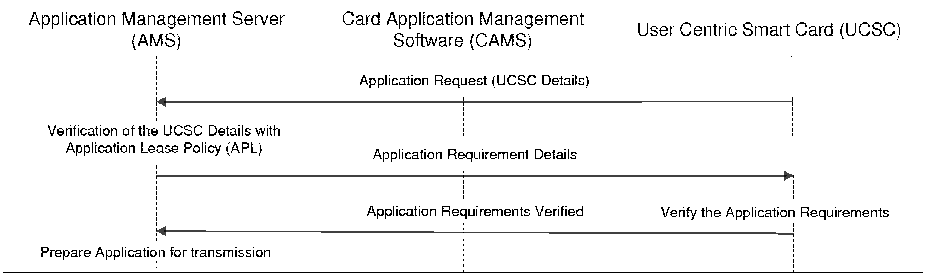

Fig. 3. Illustration of Requirement Verification Phase

application and the on-card security policy requirement includes the required firewall and application access configuration. The firewall configuration defines the mechanism through which an on-card application(s) can access (share) the requested application. The application access configuration details the mechanism through which an off-card application communicates with the application. In addition, the AMS specifies the generation requirement for the domain management key, application download key and algorithm used to encrypt the application for transmission.

The AMS and UCSC can negotiate the application communication protocol. The AMS can decide whether to use any of the UCSC implemented (open) protocols. Once the trust relationship is established and domain keys are generated, any protocols (including the GlobalPlatform) can be used to download the application on to the smart card. The AMS can also opt for their proprietary protocol to download the application. This can be achieved by first using the UCSC supported protocols to download a proprietary (small) application referred to as Application Download Manager (ADM), to a least privilege domain; the ADM will manage the download of the request application. The lease privilege domain is controlled by the UCSC, and it is a temporary domain. Applications installed in this domain are not allowed to communicate with any other applications on the smart card, which means they are in an isolated domain. The security measures will ensure that the ADM will abide by the policy of the UCSC. Before the ADM starts the execution, it will be subjected to security tests on the card to achieve the assurance that the download manager is secure and reliable to execute. During the download process, if the ADM performs any unauthorised action, the UCSC will terminate its execution and deleted it. After the application is successfully downloaded, the ADM will be deleted.

The smart card will examine the application requirement sent by the AMS. If it meets these requirements, it will send an acknowledgement to AMS and proceed to the domain creation process; otherwise, it will terminate the process.

4.1.2 Domain Creation. After the AMS and UCSC have verified each other's requirements, the next phase is to create a domain (SP's Domain), involving the following steps:

1. Allocate memory space for the SP's Domain in the EEPROM [10] (Electrically Erasable Programmable Read Only Memory).
2. After the allocation of memory space, a domain manager is installed in the allocated memory. A domain manager maintains the security aspects of the domain. Its functions are similar to a security domain in the GlobalPlatform [9]. An SP will have a view of their domain as a complete smart card.
3. After a domain is created, the Domain Delegation keys are generated. These keys can be generated in one of the following ways:
   - Either an UCSC or an AMS will generate the key and exchange it.
   - Alternatively, an UCSC and AMS can mutually generate them.

   Which of the above methods is going to be used is negotiated in the requirement verification process (i.e. section 4.1.1). Any requirements regarding the generation of the keys is solely based on SP's discretion and UCSC will follow these guidelines.

4.1.3 Downloading. After generation and mutual authentication of the Domain Delegation keys, the AMS and UCSC will start the application downloading process, shown in figure 4. An AMS will prepare the application(s) for transmitting it to the requesting UCSC. The application consists of multiple modules with varying security and operational requirements. The grouping of the application into modules of varying security and operational requirements is referred to as Application Level Modularity (ALM). Each application (i.e. banking, telecom, transport) can be divided into small modules with vary security requirement. Each application have some operational and security program code and data. These modules simply represent these logical divisions but on the line of sensitivity to the service provider. The exact framework and implementation guidelines of ALM are beyond the scope of this paper. However, for the application download process, each of the modules (i.e. group, level) of an application is encrypted with different key, and these keys are only revealed to the UCSC in incremental fashion after it satisfied the module's security and operational requirements.

The AMS will digitally sign the application with the corresponding SP's signature key, then encrypt with the transmission key. The transmission key is generated during the step three of section 4.1.2. After this the application it is transmitted to the UCSC.

The Application Download Handler (ADH) module in the UCSC handles the incoming packets. The ADH supports different application download protocols (implemented by card manufacturer). The AMS either selects one of the supported protocols or opts for its own protocol. If the SP's opt for its own protocol then the ADM (section 4.1.1) handle the application download process. The function of the ADH is to efficiently download the application in a secure and reliable fashion. The received packages of the application are not installed, because they first require the application signature validation and decryption. Therefore, downloaded applications are stored in a temporary space (in either EEPROM or RAM [10]).

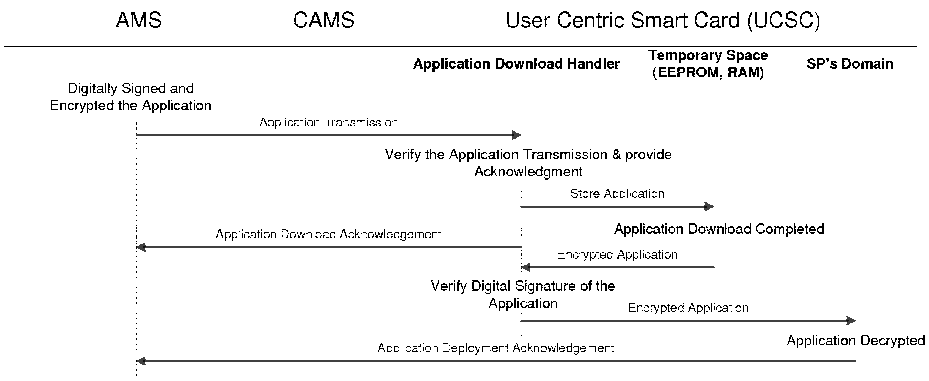

Fig. 4. Downloading an Application on an UCSC

After the download is completed, the digital signature of the encrypted application is verified. After verification of the digital signature the application is transferred to the SP's Domain and the application is decrypted there. A decrypted application is not a fully installed application. It is the equivalent of copying an application in a memory location. The decrypted application cannot be executed unless it satisfies the application verification test, discussed in the next section.

4.1.4 Application Verification by Smart Card. After an application is downloaded into the SP's domain, the next step is to verify whether the application complies with operational and security policy of the UCSC or not. A UCSC's operational and security policy defines the sanctioned operations, privileges and runtime environment restrictions on the SP's domain. To verify whether an application code conforms to specification and standards (i.e. Java Card [7], Multos [8], etc), a byte code verification is performed [17].

The byte code verification will take place on the smart card for security reasons. Performing byte code verification on the CAMS will be much faster, because in most cases it would be hosted on computationally faster machines. However, this violates the security requirement of the SP, because for a CAMS to perform byte code verification, the decrypted application would have to be transferred out of the UCSC.

The scope of this paper is not to define a byte code verifier; however, there are several well defined on-card byte code verification proposals [18, 19, 20].

4.1.5 Localisation. The application is allowed to execute on the UCSC only after it is properly verified by the UCSC. On its first execution, the application registers its security policy details with the card's security services (i.e. firewall, access manager, SP's domain manager, cryptographic services etc.). Furthermore, it may require access to specific logical or physical (i.e. contact, contactless

or web server) channels. The application will register with the communication handler (service that handles communications in and out of an UCSC) and the UCSC's application manager that allows application to be selected by an off-card entity's. Once the registration is complete, is the application is considered installed and could be accessed by an off-card entity.

4.1.6 Personalisation. After localisation is completed, the SP's application will initiate the personalisation process. The personalisation data (i.e. user's specific data) is downloaded with the application; however, it is separately encrypted. The process is as listed below.

1. An SP's application creates a message that contains on-card test and localisation process response. In addition, it generates a message for application personalisation request.
2. The AMS verifies the on-card test and localisation message. If verified it will generate the message containing the cryptographic key and digital signature on the encrypted personalisation data and it sent to the smart card. On failure the AMS will terminate the process and the smart card will delete the application.
3. The UCSC decrypts the personalisation data and verifies the digital signature. If the verification fails then the UCSC request the download again. However, if the signature verification fails after multiple tries (depending upon the UCSC's policy) then the process is terminated and the application is deleted.
4. An acknowledgement message is generated to verify to the AMS that the application is personalised successfully.
5. The AMS verify the acknowledgment message and initiate the next phase (i.e. application registration).

4.1.7 Application Registration by an AMS. The final stage of an application installation on an UCSC is the application registration by the AMS. In this stage, the AMS will register the UCSC as authorised card to an Application Lease Database (ALD) hosted on the Application Services Access Server (ASAS). After the completion of this process, the UCSC will be ready to access the SP's services.

In the UCOM, applications can be installed on one or more cards. Actually, the SP will decide whether they will allow the user to keep their application on multiple cards or not (i.e. Application Lease Policy). For certain applications, being on multiple cards would not be an issue like banking application (as it requires PIN to use the card. Therefore, if a person provides the correct PIN and it posses the appropriate application in his UCSC that means the owner was present at the point of transaction).

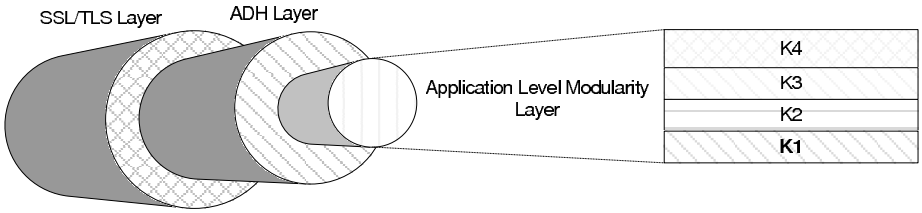

Fig. 5. Secure Communication Channel between an AMS and a Smart Card

5 Critique of the Framework

In this section, we will critically analyse the Application Management Framework in terms of its feasibility, practically and overall security perspective.

5.1 Security Analysis of the Framework

The most crucial and sensitive operation in the Application Management Framework is the application installation process. In this process, the application is transmitted over an insecure network from an AMS to a User Centric Smart Card (UCSC). The figure 5 illustrates the security envelopes on the application in transit over an insecure network.

The top envelope is provided by the two-way SSL/TLS session established directly between an UCSC and an AMS. During the second phase (i.e. Domain Creation) of the installation process, the Domain Delegation keys are generated. Along with these keys the Application Installation key (i.e. transmission keys) are also generated that are used by the Application Download Handler (ADH) to securely download the application from its respective SP. The Application Installation keys are only used once, at the time of installation and then they are securely discarded. During the deletion process, an SP only needs to use their Domain Delegation keys to instruct the deletion command to their application. The final layer of protection in the application installation process is provided by Application Level Modularity (ALM). In ALM each group of modules with the same security association and requirements would be encrypted separately with different keys, and each of the keys are only provided to an UCSC after it satisfies the associated requirements for the module level. Therefore, an application has at least three security layers for the secure communication on the insecure network during the installation process, as shown in the figure 5. An obvious attack can be to reset an UCSC with weak security provisions (i.e. SSL/TLS key pair, domain key generation mechanism etc). However, an SP will always have the right to deny any UCSC that cannot satisfy its requirements. Therefore, the SP has to be sure of security measures implemented by the UCSC before it leases its application. This assurance is provided by the Common Criteria Security Evaluation Certificate, UCSC manufacturer certificate and self testing or state assurance mechanism (i.e. Trusted Platform Module in SE).

In addition, attacks like fault attacks or Side-channel attacks [21] on a smart card can be mounted against an UCSC. As a protection measure against the fault attacks during the installation/deletion process (either to corrupt the UCSC or the application to retrieve sensitive data), the UCSC will be in defensive mode. The defensive mode enables an UCSC to save the secure, operational and reliable state of the UCSC before proceeding with the installation process. In addition, the UCSC intercepts each instruction and determines whether the execution of the instruction will violate the safe state of the UCSC or not. If it is safe to execute, it will allow the instruction to be carried out; otherwise, it will terminate the process. If anything goes wrong, the UCSC aborts the installation process and reset to the safe state (saved before the process initiated. The safe state of the smart card represents the state of the operational, and security modules (i.e. Firewall, Access Controller, Communication Channels, Execution Environment) of the UCSC that are responsible for the smart card platform reliability and security. The defence against the side channel attacks is mostly implemented on the hardware layer. Therefore, Common Criteria Security Evaluation Certificate will test the security mechanisms that provide protection against the Side-Channel attacks. If a service provider does not accept the certificate, the process will be terminated. The SPs are in total control of their applications and they have the sole discretion whether to lease or deny the lease request, this assures the service providers that their application will only be installed on an UCSC that meets their ALP, after their authorisation.

5.2 Operational Critique of Framework

The User Centric Smart Card Ownership Model (UCOM) emphasise on delegating the ownership of the smart card to its user. Therefore, the framework that supports the UCOM proposal has to be user friendly and less complex. The application installation, especially on the smart card, is technically challenging. Therefore, the proposed Application Management Framework (AMF) performs majority of the processes without the cardholder's interaction. It will be less prone to errors if the user interaction during the application management processes is limited.

As a result of the recent technological developments in mobile handsets (i.e. Near Field Communication), there is a renewed interest by large scale horizontal industries (i.e. banks, transport and telecom operators) in the multi-application smart card initiative. The UCOM capitalises on the development and gives the opportunity to small organisation to develop applications that can be deployed on their user's UCOM supported NFC enabled mobile phones. The framework proposed in the paper does not rely heavily on telecom operators. The basic requirement is to establish an internet connection with the service provider's Application Management Server (AMS). This can be achieved through connecting to the internet by wireless internet, Bluetooth or cable connection (by connecting the mobile phone with a personal computer). The overall framework would not require any change to cope with different intermediary networks (protocols) that establish a connection with the service provider's AMS. In certain situations

(i.e. small organisations, home environment), there is no need to set up AMS and connect the UCOM-based smart card through internet. In such cases the user can actually install the application, by directly connecting with the AMS without an internet. The only change to the framework is on the Card Application Management Software (CAMS) that has to connect to a local computer through any of the supported bearers (i.e. Bluetooth, wireless, USB). This makes the UCOM capable of being deployed in local environments that are difficult to achieve in the SE management framework that relies on Trusted Service Manager (TSM). Possible applications in the local environments can be access controller (i.e. doors, car, computers), home appliance management application (controls the intelligent kitchen, home appliances), utility meters payment/management, local library, school/college and local grocery stores application etc.

6 Future Research Directions

This paper should not be considered as one that has solved all of the issues relating to the UCOM or the AMF. The issues that are still not resolved are listed in this section.

- Common Criteria Security Evaluation Certificate: The Common Criteria do not stipulate a security certificate on the smart card itself. The certificate discussed in the paper provides an assurance of security from the neutral security evaluators. SPs can rely on their evaluations to verify the security claim of the UCSC. Further research is required in the security evaluation certificate mechanism and how they can be integrated with other components (i.e. TPM) on an UCSC to provide security assurance to SPs.
- Firewall: Firewall designs of modern smart cards are based on the presumption that the smart card is under complete control of the card issuer. Due to this assumption, the firewall is designed from the point of view of what can be shared. Therefore, traditional firewall mechanism in the smart cards may not be adequate for the UCOM.

7 Conclusion

In this paper, a framework is presented for application management in the User Centric Smart Card Ownership Model (UCOM). The operations preformed by the smart card and Application Managment Server (AMS) are provided and such operations are possible with the present state of the technology as most of these measures are already implemented to support other mechanisms. In addition this paper also provides the associated issues that are required to be resolved to fully explore the user's ownership model. Further work will be conducted in order to attempt to answer the pointes mentioned in the future research directions.

References

1. "Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications," White Paper, November 2006.
2. "The GlobalPlatform Proposition for NFC Mobile: Secure Element Management and Messaging," GlobalPlatform, White Paper, April 2009.
3. "Near Field Communications (NFC). Simplifying and Expanding. Contactless Commerce, Connectivity, and Content," ABI Research, Oyster Bay, NY, 2006.
4. "Pay-Buy-Mobile: Business Opportunity Analysis," GSM Association, White Paper 1.0, November 2007.
5. "Co-Branded Multi-Application Contactless Cards for Transit and Financial Payment," Smart Card Alliance, NJ. USA, White Paper, March 2008.
6. "Mobile NFC Services," GSM Association, White Paper Version 1.0, 2007.
7. Java Card Platform Specification; Application Programming Interface, Runtime Environment Specification, Virtual Machine Specification, Sun Microsystems Inc. Version 2.2.2, March 2006.
8. "Multos – http://www.multos.com/."
9. GlobalPlatform: GlobalPlatform Card Specification, Version 2.2, GlobalPlatform, March 2006.
10. W. Rankl and W. Effing, Smart Card Handbook. New York, NY, USA. John Wiley & Sons, Inc., 2003.
11. T. Dierks and E. Rescorla, Eds., The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346., 2006. http://tools.ietf.org/html/rfc4346
12. D. E. Comer, Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture, 4th ed. Prentice Hall, January 2000.
13. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. CRC, October 1996.
14. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements, Common Criteria. Version 3.1, August 2006.
15. Trusted Module Specification 1.2: Part 1- Design Principles, Part 2- Structures of the TPM, Part 3- Commands, Trusted Computing Group, Rev. 103, July 2007.
16. Smartcard-Web-Server, Smartcard Web Server Enabler Architecture, Smartcard Web Server Requirements,, Open Mobile Alliance (OMA), 2008.
17. L. Casset, L. Burdy, and A. Requet, "Formal Development of an Embedded Verifier for Java Card Byte Code," in DSN '02: Proceedings of the 2002 International Conference on Dependable Systems and Networks. Washington, DC, USA: IEEE Computer Society, 2002, pp. 51-58.
18. G. Barthe, G. Dufay, L. Jakubiec, and S. Melo de Sousa, "A Formal Correspondence between Offensive and Defensive JavaCard Virtual Machines," in VMCAI '02: Revised Papers from the Third International Workshop on Verification, Model Checking, and Abstract Interpretation. London, UK: Springer-Verlag, 2002, pp. 32-45.
19. D. Deville and G. Grimaud, "Building an "impossible" verifier on a java card," in WIESS'02: Proceedings of the 2nd conference on Industrial Experiences with Systems Software. Berkeley, CA, USA: USENIX Association, 2002, pp. 2-2.
20. X. Leroy, "Bytecode verification on Java smart cards," Softw. Pract. Exper., vol. 32, no. 4, pp. 319-340, 2002.
21. P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer-Verlag, 1999, pp. 388-397.