A Person-to-Person Internet Payment System

Mansour A. Al-Meaither and Chris J. Mitchell
Information Security Group, Royal Holloway, University of London,
Egham, Surrey TW20 0EX, UK.
M.Al-meaither@rhul.ac.uk, C.Mitchell@rhul.ac.uk

Abstract

As Internet commerce becomes widely used between individuals, the need for interpersonal payment schemes will grow. In this paper we propose a new Internet person-to-person payment system that is both secure and efficient. After describing a general model for interpersonal Internet payments, we consider the associated security risks. Security requirements are identified for a person-to-person Internet payment system. We then present a payment protocol designed to address the identified security requirements and describe the various phases that comprise the payment protocol. Finally, we analyse how the proposed protocol matches the identified security requirements.

Keywords:

Internet, E-commerce, payment systems, security, public key cryptography.

1 Introduction

One critical enabler of e-commerce transactions is secure Internet payments. The importance of Internet payment systems is increasing rapidly as e-commerce becomes part of our ordinary daily life. Internet payment protocols incorporating cryptographic measures are of potentially great importance in preventing large-scale fraud. Currently, most Internet payment protocols can be categorised by the identity of the participants into:

- Business-to-consumer (B2C) payment protocols using payment cards, e.g. *i*KP [5], SET [10],
- Business-to-business (B2B) payment protocols, e.g. e-check [4].

Payment cards are a simple way for people to pay businesses for products and services, but they do not provide private individuals the means to pay each other (here, private individuals means consumers and non-professional merchants). For example, a private seller who wants to obtain permission to accept credit-card payments has to apply for a merchant processing account, which can cost him up to 5% of a transaction to have it processed. However, this might not be cost effective for person-to-person transactions.

On the other hand, cheque payments are still used heavily between individuals. In its annual report [6], APACS indicated that cheque payments in the UK increased in 1999, mainly due to rises in person-to-person payments and credit card repayments.

The dominance of the cheque for making person-to-person payments in the Internet has associated problems. A recent survey of online auctions performed by the National Consumers League [7], found the following complaints about payments between buyers and sellers:

- 34% of sellers complained of late buyer payments,
- 27% of sellers never received payment, and
- 5% of buyer cheques bounced.

The current situation can be changed if a new Person-to-Person (P2P) Internet payment system can be devised. This new payment system will need to conform to current user practices, use existing payment infrastructures, and have minimum impact on buyers, sellers, banks, and the financial system.

Thus, there are two main reasons for considering a novel P2P Internet payment system:

- Such a scheme will create new markets since it will create new opportunities for individuals to engage in private e-commerce, ranging from classified advertisements to auctions and home businesses;
- There are potentially significant cost savings to the end users and banks.

2 Using existing banking relationships for P2P payments

It is difficult for people unknown to each other to perform e-commerce transactions unless they possess credentials from a trusted common source. Although many people have no way to authenticate and validate each other over the Internet, many have bank relationships. APACS estimates that 83% of adults in the UK hold a current account with a bank or building society [6]. It should therefore be possible to devise a P2P payment system that uses the buyer and seller banks. In such a system the buyer authorises payment from his bank, the seller verifies payment has been received by his bank, and the seller then supplies the goods to the buyer. The seller will be able to see if the buyer has enough funds by debiting the buyer account in real time and provide the buyer with the ability to complete transactions using the existing trusted relationship with their banks. This idea motivates the remainder of this paper.

3 Person-to-person Internet Payments Model

In this section, we describe our model of an interpersonal payment system. The model identifies the entities involved and give a brief description of their interactions.

3.1 Entities involved

A person-to-person Internet payment system as shown in Figure 1 involves interactions between: the buyer, the seller and a trusted third party, which we call the "Payment Gateway", together with the buyer and the seller banks. Their roles are straightforward.

- **Buyer**: This is the entity that makes the payment in exchange for goods or services using money in his bank account. The buyer has a digital certificate issued by the trusted payment gateway that links his bank account with his public key.
- **Seller**: This is the entity that receives money from the buyer during a payment transaction in return for providing the buyer with goods or services. The money is deposited into his bank account. Although the seller trusts the payment gateway, the buyer and the seller need not trust each other. The seller has a digital certificate issued by the payment gateway that links his bank account with his public key.
- **Payment Gateway**: This is a trusted third party which links electronic payments to the transfer of "real money". It certifies the trustworthiness of the buyer and the seller by issuing, maintaining and validating digital certificates that link the seller (buyer) bank account to his public key. Every participant must have his own certificate for the system to work. The payment gateway and the buyer's bank are assumed to enjoy a degree of mutual trust and share an infrastructure for secure communication, i.e. the financial network. In the event of a dispute, the payment gateway shall be capable of producing proof of buyer authorisations to the buyer bank. The payment gateway shall store those authorisations securely. To minimize the risks of attacks from hackers, the payment gateway should not store the buyer or the seller bank account number. If necessary, it communicates with the banks to confirm seller/buyer account numbers.
- **Buyer Bank**: This is a financial institution that establishes an account for a buyer. It trusts the payment gateway to pass it buyer-approved payment instructions. The buyer has authorized his bank to accept payment gateway messages. It must be able to show the destination of the transferred money if needed.
- **Seller Bank**: This is a financial institution that establishes an account for a seller. It accepts money transfers made by buyers and credits them to the seller account. It must be able to show the source of the transferred money if needed.

3.2 Interactions

In our payment model, the seller sends his bank account number and the goods description in a seller block SBLK to the payment gateway, which certifies the correctness of the account number by creating a certified seller block CSBLK. The concept of seller block SBLK is introduced here to give the buyer confidence that the seller he is dealing with is genuine. Every time a seller agrees with a buyer on the sale of specific goods, he should generate an SBLK that is specific

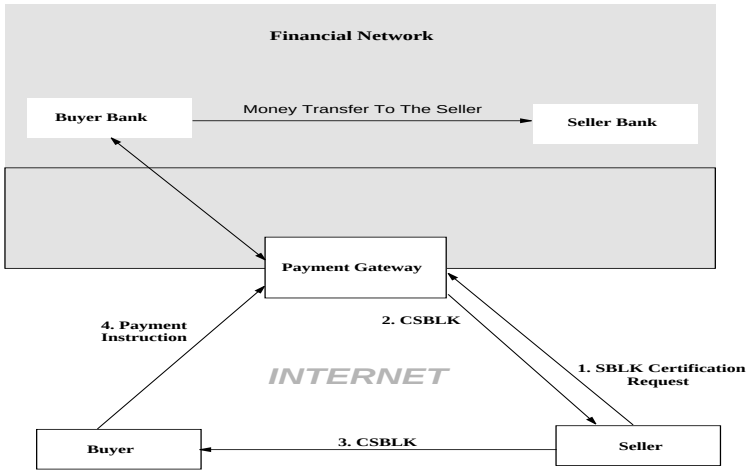

Figure 1: **System model for a P2P Internet payment system**

to this transaction and incorporates the agreed price. The seller must then have it certified by the payment gateway to produce the certified seller block CSBLK. The seller then sends (or makes available) this CSBLK to the buyer who uses it to instruct the payment gateway to pay the seller using his bank account. A payment to a seller will only be successful with the presence of a valid CSBLK. Once the payment gateway has received a valid payment instruction from the buyer, it communicates with the buyer bank to instruct it to transfer the agreed payment for the goods from the buyer account to the seller account.

4 Security Risks

The most likely motive for any fraudulent attack would be financial gain. This could be accomplished by creating fraudulent electronic representations of the payment instruction that are accepted as genuine by the payment gateway, or by stealing data from another participant. If successful this would cause financial loss to the buyer bank or other participants. Alternatively, an attack on a person-to-person Internet system might be motivated not by financial gain but by a desire to disrupt a particular system. An important aspect of the vulnerability of person-to-person Internet payment system is that it must be designed for widespread use. Thus, it must be assumed that it would not be difficult for an attacker to repeatedly attempt to compromise the system. The primary areas of vulnerability in a person-to-person Internet payment system are the computers used in the system, and the messages transmitted between the participants.

4.1 Alteration of data in computers

The objective of fraud could be to modify the seller bank account number stored on the seller computer in an unauthorized manner. For example, if the seller bank account number were fraudulently changed without other evidence of tam-

pering, the buyer could pay an attacker who would appear genuine to the buyer.

4.2 Alteration of messages

An attacker could attempt to delete messages, replay messages, substitute an altered message for a valid one, or observe messages for the purpose of attempting an attack. Critical data in a message, such as the price, could be changed and the message then retransmitted to its intended recipient. Messages authorising the payment of money could be copied and replayed to the payment gateway in an attempt to receive double credit for the transactions.

4.3 Theft

A straightforward method of attack would be to steal a buyer computer and fraudulently utilize the data stored on the computer. For example, an attacker could intercept messages between a genuine buyer and a payment gateway, or insert unauthorized software into a buyer's computer that enabled the attacker to copy payment instructions stored or in transmission, and then use the payment instructions to perform transactions. Such a theft would only be detected after the payment gateway (or buyer bank) received both the fraudulent and the genuine copy of the same payment, by which time the attacker would probably already have obtained financial benefit.

Internal theft within a payment gateway could also be a means of attack. One significant threat to the system would be the theft or compromise of the payment gateway's cryptographic keys by either an inside or an outside attacker.

4.4 Repudiation of transactions

Fraud could also be attempted through repudiation of transactions. For example, a buyer could fraudulently claim to his bank that he had not authorised a particular transaction. This could cause losses to the payment gateway.

4.5 Breach of user privacy

An interceptor of transaction messages could learn the identity of the buyer, as well as details of the transaction (e.g. price, nature of goods, etc.). In some circumstances this would be an undesirable breach of user privacy.

5 Security Requirements

We next consider what security services are required to combat the threats identified in the previous section.

5.1 Confidentiality

1. The buyer needs to keep his payment information secret from the seller and outsiders.

5.2 Authentication

This security service can be sub-divided into the following.

1. The seller needs to authenticate the payment gateway to prevent transmission of the SBLK to an attacker.
2. The buyer needs assurance that the seller is accredited at the payment gateway. Otherwise he might be paying an attacker.
3. The buyer needs assurance that he is sending the payment instruction to the real payment gateway.
4. The payment gateway needs to authenticate the buyer to prove that he is the legitimate owner of the payment instruction received.
5. The payment gateway needs to authenticate the seller whose bank account number is in the payment instruction sent by the buyer.

5.3 Integrity

Integrity should give assurance that buyer money is not taken without his authorisation.

1. The buyer requires a proof that the seller specified in the CSBLK received the payment, to protect against repudiation by the seller.
2. Even if the seller is an adversary, nobody should be able to present a false payment instruction to the payment gateway on behalf of a buyer.
3. When the payment gateway requests the buyer bank to debit a buyer account by a certain amount and credit it to the seller account, the payment gateway must be in possession of a proof that the buyer has authorised this payment in order to protect itself against repudiation by buyer.
4. The SBLK contents must be protected against alteration, or any alteration must be detectable.

6 The Protocol

We now describe the proposed person-to-person Internet payment protocol in detail. This protocol conforms to the model shown in Figure 1.

It consists of three phases: *the Registration phase*, in which the payment gateway registers the participant and issues him a digital certificate that binds his bank account to his public key; *the Seller Block Certification phase*, invoked by the seller, wherein the payment gateway certifies that his bank account number matches his identity, and *The Payment phase* invoked by the buyer, wherein the buyer validates the seller bank account number and sends authorisation to his bank to transfer the agreed amount of money from the buyer bank account to the seller's bank account.

An important advantage of this system is its auditability. Once a payment transaction has finished, the buyer can determine who authorized the payment, and that the payment transaction was credited to the seller bank account. In

addition, the model is resistant to fraud because the payment gateway will accept payment instructions only from the buyer himself, so it only has to authenticate that it is talking to the person who owns the account being charged, and it does not have to rely on any other party. However, a disadvantage of this model is that the seller must receive a payment confirmation. Guarantee of Payment to the seller is clear in this system since the buyer will ask the payment gateway to instruct his bank to transfer the specified amount of money to the seller bank account, which could be an immediate transfer or might take some time. In the latter case, the payment gateway has already received a positive response from the buyer bank, which is a payment guarantee for the seller and allows him to ship the goods. The payment gateway provides liability protection for the seller because it provides him with proof that the buyer bank has authorized the payment to the seller bank account.

6.1 Data Items

Table 1 summarises the notation used for the cryptographic functions and keys held by the participants in the protocol. Note that in this table, as throughout, || is used to denote concatenation of data items.

Table 1: **Notation used in the protocol descriptions**

Notation	**Description**
B	The Buyer.
BBLK	Buyer block = buyer bank account number || goods description || price.
Cert_{P_X}	A certificate for the public encryption key of entity X (i.e. P_X), issued by the Payment gateway.
Cert_{V_X}	A certificate for the signature verification key of entity X (i.e. V_X) issued by the Payment gateway.
CSBLK	certified seller block = authenticated SBLK (see section 6.2.3).
$e_{P_X}(M)$	The public key encryption of message M using the public key of entity X (P_X).
h	A collision-free, one-way hash function (e.g. SHA-1 [1]).
ID_X	A string of bits that uniquely identifies entity X within the domain of application of the protocol.
PG	The Payment Gateway.
P_X	The public encryption key of entity X.
R_i	Random nonce, $i = 1, 2, 3, \ldots$
result	One bit indicating whether the payment completed or failed.
S	The Seller.
S_X	The private signature key of entity X.
$s_{S_X}(M)$	The signature on message M using the private signature key of entity X. We assume that M can be recovered from the signature— if not, then the notation implies that a copy of M is sent with the signature.
SBLK	Seller block = nonce || goods description || price || seller bank account number.
T	Time stamp.
V_X	The public signature verification key of entity X.

The Seller block SBLK is an important data item in the person-to-person Internet payment system. It provides for the payment to be made to the seller's bank account. Every time a seller wants to sell goods, he should generate an SBLK and have it certified by the payment gateway to produce the certified seller block CSBLK.

6.2 Protocol Description

Our protocol consists of 3 phases:

1. The Registration phase,
2. The Seller Block Certification phase, and
3. The Payment phase.

Both the Seller Block Certification phase and the Payment phase protocols conform to the mutual entity authentication mechanism using digital signature techniques specified in clause 5.2.2 of ISO/IEC 9798-3 [3], they are also both similar to the protocol proposed in [8].

6.2.1 Specific Requirements

In order to execute the protocol, the following requirements must be satisfied.

1. The buyer, the seller and the payment gateway must have the means to generate unpredictable random numbers R_i.
2. The buyer, the seller and the payment gateway must be using the same digital signature scheme, asymmetric encryption scheme, e.g. RSA [9], and hash function, e.g. SHA-1 [1].
3. The payment gateway and the seller must have securely synchronised clocks, in order to be capable of generating and verifying timestamps.
4. Each participant X must have two asymmetric key pairs: one pair used for encryption and decryption and the other (S_X, V_X) used for the creation and verification of digital signatures. This requirement applies not only to buyers and sellers but also to the Payment Gateway.

6.2.2 Registration phase

In this phase a user X registers with the payment gateway and obtains its own public key certificates. All users, both buyers and sellers, must register before participating in the system. The payment gateway issues X.509 certificates [2] that contain the user (unique) bank account number. In order to make use of the bank's existing ability to authenticate their customers, the payment gateway may employ the user bank as a Registration Authority. The payment gateway will reissue the certificate upon expiry, provided that the bank account is in good standing and that no theft or misuse of the signer's private signature key has been reported. The X.509 certificate only informs the signature verifier that the public key is legitimately associated with a signer and a valid bank account at the time that the certificate was issued. This phase has three steps:

1. $X \leftrightarrow PG$: Authenticate ID_X
2. $X \rightarrow PG$: Bank account number, P_X, V_X
3. $PG \rightarrow X$: Cert_{P_X}, Cert_{V_X}, P_{PG}, V_{PG}

First, payment gateway PG securely confirms that user X has identifier ID_X. Then, user X sends public keys P_X and V_X, and his bank account number to the Payment Gateway PG. After verifying the association between the entity and the supplied bank account, Payment Gateway signs and sends two public key certificates Cert_{P_X}, Cert_{V_X} for the supplied user keys to the user, along with its public keys P_{PG} and V_{PG}. After this phase, both the buyer and the seller have trusted copies of the payment gateway's public encryption key and public signature verification key. The payment gateway does not have to store any copies of the buyer and the seller keys.

6.2.3 Seller Block Certification phase

Once the seller and the buyer have agreed on the goods to be sold and the price, the seller will begin the process of creating the SBLK for that sale and have it certified by the payment gateway to produce a certified seller block CSBLK. CSBLK is introduced to give the buyer confidence that the seller he is dealing with is genuine and to allow the payment gateway to check the seller certificate for revocation and expiry. A CSBLK contains information related to the goods being sold and the seller bank account number. Every time a seller wants to sell goods, he should generate a SBLK that must be certified by the payment gateway to produce a CSBLK.

This phase has four steps. S initiates a communication session with PG. He chooses and sends a random number R_1, his public encryption key certificate and the SBLK which contains sale information and the seller bank account number. This will indicate to the payment gateway that S is willing to begin a seller block certification process. In order to protect the SBLK contents from eavesdroppers, the SBLK is encrypted under the public encryption key of the payment gateway.

1. $S \rightarrow PG$: $R_1 \parallel e_{P_{PG}}(\mathrm{SBLK} \parallel \mathrm{Cert}_{P_S})$

Once it is has received the message in step 1, PG chooses and sends a random number R_2 to S along with its signature on the concatenation of the random number R_1 sent by S, its own random number R_2, the seller identifier ID_S and the SBLK received in step 1 above, all encrypted under the public encryption key of the seller sent in step 1.

2. $PG \rightarrow S$: $e_{P_S}(R_2 \parallel s_{S_{PG}}(R_2 \parallel R_1 \parallel \mathrm{ID}_S \parallel \mathrm{SBLK}))$

After receiving the message in step 2 and successfully verifying the Payment Gateway's signature, S knows now that he is talking to PG in real time. S signs the concatenation of random numbers received in step 2, the PG identifier ID_{PG} and the seller block and send it along with its signature verification digital certificate Cert_{V_S} to PG, all encrypted under the public encryption key of the payment gateway.

3. $S \rightarrow PG: \quad e_{P_{PG}}(s_{S_S}(R_1 \parallel R_2 \parallel \mathrm{ID}_{PG} \parallel \mathrm{SBLK}) \parallel \mathrm{Cert}_{V_S})$

After receiving the message in step 3 and successfully verifying the seller's signature, PG knows that it is talking to the seller whose identifier is ID_S. Next, using the financial network, the payment gateway will make sure that the bank account number found in SBLK belongs to the identified seller. Once these checks have successfully been completed, it creates, encrypts and sends to the seller, $\mathrm{CSBLK} = s_{S_{PG}}(T \parallel \mathrm{ID}_S \parallel \mathrm{SBLK})$. CSBLK can be used by the buyer to pay the seller the agreed price for the specified goods, and the seller uses CSBLK to indicate to the buyer that he is the genuine seller. The time stamp T indicates the expiry time of the CSBLK.

4. $PG \rightarrow S: \quad e_{P_S}(T \parallel s_{S_{PG}}(T \parallel \mathrm{ID}_S \parallel \mathrm{SBLK}))$

6.2.4 The Payment phase

After the buyer and the seller have agreed on the goods and price, the seller will make the CSBLK available to the buyer by some means, e.g. by email or through the seller site. The buyer then will send the CSBLK to the payment gateway for verification. If the verification process succeeds the Payment Gateway will then debit the buyer account and credit the seller account.

This phase has five steps.

Once B has a copy of the CSBLK, it will start communicating with PG. B chooses and sends a random number R_3, his public encryption key certificate and the buyer block information BBLK, which contains the sale information and the buyer bank account number. In order to protect the BBLK contents from eavesdroppers, the BBLK is encrypted under the payment gateway public key P_{PG}.

1. $B \rightarrow PG: \quad R_3 \parallel e_{P_{PG}}(\mathrm{BBLK} \parallel \mathrm{Cert}_{P_B})$

On receiving the message in step 1, PG chooses and sends a random number R_3 to B along with its signature on the concatenation of the random number R_3 sent by B, its own random number R_4, the buyer identifier ID_B and the BBLK received in step 1, all encrypted under the public encryption key of the buyer sent in step 1.

2. $PG \rightarrow B: \quad e_{P_B}(R_4 \parallel s_{S_{PG}}(R_4 \parallel R_3 \parallel \mathrm{ID}_B \parallel \mathrm{BBLK}))$

After receiving the message in step 2, B knows that he is talking to PG in real time. Now he instructs the payment gateway to communicate with the buyer bank to transfer the amount specified in the CSBLK from his account to the seller account. B does that by signing the concatenation of: the random numbers received in step 2, the PG identifier ID_{PG}, the buyer block BBLK, the time the payment is made T, and the CSBLK. Then, B sends this along with its signature verification digital certificate Cert_{V_B} to PG, all encrypted under the public encryption key of the payment gateway.

3. $B \rightarrow PG: \quad e_{P_{PG}}(s_{S_B}(R_3 \parallel R_4 \parallel \mathrm{ID}_{PG} \parallel T \parallel \mathrm{BBLK} \parallel \mathrm{CSBLK}) \parallel \mathrm{Cert}_{V_B})$

After processing the payment instruction and receiving a positive response from the buyer bank that the money has been transferred, the payment gateway PG will send a confirmation message to both the buyer B (as in step 4) and the seller S (as in step 5) signifying the outcome of the payment using the field "*result*". Messages 4 and 5 also indicate that at time T, B has paid the amount specified in SBLK using the bank account indicated in BBLK to the seller bank account indicated in CSBLK in exchange for the goods described in CSBLK.

4. $PG \rightarrow B: \quad e_{P_B}(T \parallel s_{S_{PG}}(T \parallel result \parallel \mathrm{ID}_B \parallel \mathrm{BBLK} \parallel \mathrm{CSBLK}))$
5. $PG \rightarrow S: \quad e_{P_S}(T \parallel s_{S_{PG}}(T \parallel result \parallel \mathrm{ID}_S \parallel \mathrm{BBLK} \parallel \mathrm{CSBLK}))$

7 Security analysis

In this section, we will examine to what extent the generic security requirements outlined in section 5 are met by our protocol.

7.1 Confidentiality

The P2P protocol provides privacy for the buyer and the seller from outsiders. Confidentiality is provided using public key encryption.

7.2 Authentication

Authentication is provided using digital signatures and public key certificates issued by the payment gateway (PG).

1. The Buyer needs to authenticate the seller:
   This requirement is met implicitly, because the buyer can verify that the payment gateway has authenticated the seller by verifying the payment gateway signature found in CSBLK, i.e. $s_{S_{PG}}(T \parallel \mathrm{ID}_S \parallel \mathrm{SBLK})$.

2. The Buyer needs to authenticate the payment gateway:
   This requirement is met, because the buyer can verify the signature received in step (2) of the payment phase, using the verification key found in the payment gateway certificate.

3. The payment gateway needs to authenticate the buyer:
   This requirement is met, because the payment gateway can verify the buyer signature received in step (3) of the payment phase, using the buyer certificate. The buyer certificate issued by the payment gateway is evidence that the buyer's public key matches to the bank account number.

4. The payment gateway needs to authenticate the seller:
   This requirement is met, because the payment gateway can verify the seller signature received in step (3) of the seller block certification phase, using the seller certificate, and verify that the bank account number found in the SBLK belongs to the seller identified in the seller certificate. The seller certificate issued by the payment gateway is evidence that the seller's public key matches to the bank account number.

7.3 Integrity

1. The buyer needs Proof that the seller received the payment:
   The buyer could consider the message received in step (4) of the payment phase as a proof, since the payment gateway signs this message, in which the data item "*result*" indicates whether the payment has taken place or not. There is a possibility that the payment gateway might not send the above message even though it has already received the payment message from the buyer. In this case, the buyer does not know whether the transaction was aborted or finalized; however, the buyer can ask his bank for an account statement which can act as a replacement for this receipt.

2. Payment without buyer authorisation is impossible:
   The buyer bank account number signed by the buyer is sent in step (3) of the payment phase, and no one but the buyer has the private key necessary to make the required signature, even if there are many previous signed transactions. The only exception is if the payment gateway instructs the buyer bank to debit the buyer account without receiving buyer authorisation. In this case, the buyer can repudiate this payment by going to his bank who in turn will ask the payment gateway for buyer authorisation.

3. Payment gateway needs a proof that the buyer has authorized the payment:
   This requirement is met, because the buyer signs the message in step (3) of the payment phase, and the PG can verify the buyer signature using the buyer certificate.

4. The seller needs to make sure that the CSBLK cannot be altered:
   This requirement is met, because the CSBLK is protected by encryption during the seller block certification phase where it is transmitted to the seller. In addition, the CSBLK supplied by the buyer to the payment gateway during the payment phase must be signed by the payment gateway.

7.4 Some potential problems

- A potential problem with our proposal is that it possesses a central point of attack. The payment gateway is trusted by all participants to make trustworthy decisions about the authenticity of a participant. Compromise of the payment gateway would be disastrous. The effects of a denial of service attack on the payment gateway are also severe. Obviously, the usefulness of a system like this increases in proportion to the number of users who subscribe, although the effects of an outage (deliberate or accidental) increase. One solution to such problems of service availability is for the payment gateway to employ replication to achieve availability and to use proactive recovery with threshold cryptography for digital signature operations [11].

- Sellers should be able to refund payments to buyers if necessary, although this is not supported by the scheme as described above. However, the seller can be asked to send a digitally signed document to the payment gateway promising to repay the goods money, unless it is delivered to

the buyer. The payment gateway holds this signed statement, and thus the buyer can be guaranteed that he will be repaid if the goods are not delivered.

8 Concluding remark

The authors would like to thank an anonymous referee for a number of helpful comments and suggestions. This includes pointing out that a somewhat similar scheme to the one described in this paper is already in use in the Nordic countries, where most people have access to Internet home banking. However, important differences between the two systems do exist, and planned future research includes a detailed comparison between the properties of the two schemes.

References

[1] FIPS 180-1. *Secure Hash Standard.* National Institute of Standards and Technology. FIPS Publication 180-1, 1995.

[2] ISO/IEC 9594-8. *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.* International Organization for Standardization, Geneva, Switzerland, 2000.

[3] ISO/IEC 9798-3. *Information technology — Security techniques — Entity authentication mechanisms — Part 3: Mechanisms using digital signature techniques.* International Organization for Standardization, Geneva, Switzerland, 1998.

[4] M.M. Anderson. The electronic check architecture, version 1.0.2. http://www.echeck.org, 1998.

[5] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E. Van Herreweghen, and M. Waidner. Design, implementation and deployment of the *i*KP secure electronic payment system. *IEEE Journal on Selected Areas in Communications*, 18(4):611–627, 2000.

[6] Association for Payment Clearing Services (APACS). In brief-payment market briefing 2000. http://www.apacs.org.uk, 2000.

[7] National Consumers League. Survey of online auction goers. http://www.natlconsumersleague.org/onlineauctions/auctionsurvey2001.htm, 2001.

[8] R.M. Needham and M.D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(2):993–999, 1978.

[9] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[10] SET. *The SET Standard Book 1 Business Description*, version 1.0 edition, 1997. http://www.setco.org.

[11] L. Zhou, F. B. Schneider, and R. van Renesse. Coca: A secure distributed on-line certification authority. Technical Report 2000-1828, Department of Computer Science, Cornell University, Ithaca, NY USA, December 2000.