Project Number	AC026
Project Title	Secure Electronic MarketPlace for Europe SEMPER
Deliverable Security Class	Public
CEC Deliverable Number	AC026/SMP/CT2/DS/P/015/b1
Contractual Date of Delivery	November 30, 1997
Actual date of Delivery	December 10, 1997
Title of Deliverable	Deliverable D15
	New Payment Instruments Prototype
Contributing Workpackages	WP 2.5
Nature of the Deliverable	Specification
Author(s)	Birgit Baum-Waidner (R3), Kim Lüders-Jensen (Cryptomathic), Marc Mazoué (CNET), Thomas Mittelholzer (R3), Armin Mueller (R3), Torben Pedersen (Cryptomathic)
Editor(s)	Thomas Mittelholzer (R3), Armin Müller (R3)
Keywords	Payment Instruments, Electronic Cheques, C-SET, e-COMM, Security

SEMPER Consortium:

New Payment Instruments Prototype

Deliverable D15 of ACTS Project AC026

Public Specification
December 10, 1997

SEMPER is part of the European Commission's ACTS Programme (Advanced Communications Technologies and Services). Funding is provided by the partner organisations, the European Union, and the Swiss Federal Department for Education and Science.

The members of the SEMPER consortium are Commerzbank (D), Cryptomathic (DK), DigiCash (NL), EUROCOM EXPERTISE (GR), Europay International (B), FINTEL (B), FOGRA Forschungsgesellschaft Druck (D), France Telecom - CNET (F), GMD - German National Research Center for Information Technology (D), IBM La Gaude (F), IBM Zurich Research Lab (CH), INTRACOM (GR), KPN Research (NL), MARIS (NL), Otto-Versand (D), r3 security engineering (CH), SINTEF Telecom and Informatics (N), Stichting Mathematisch Centrum / CWI (NL), University of Freiburg (D), University of Dortmund (D) (having replaced University of Hildesheim (D)), University of Saarbruecken (D), Banksys (B), Banque Générale du Luxembourg (L) and Telekurs (CH) are associated with SEMPER.

For more information on SEMPER visit

<http://www.semper.org>

or contact

Gerard Lacoste
IBM La Gaude
Centre d'Etudes et Recherches
Le Plan du Bois
F-06610 La Gaude, France

Phone + 33 92 11 48 07
Fax +33 93 24 45 45
Mail lacoste@vnet.ibm.com

Michael Waidner
IBM Research Division
Zurich Research Laboratory
Säumerstrasse 4
CH-8803 Rüschlikon, Switzerland

Phone +41 1 724 8220
Fax +41 1 710 3608
Mail wmi@zurich.ibm.com

Management Summary

The main objective of *SEMPER* (Secure Electronic MarketPlace for Europe) is to develop, implement and evaluate by trials an open security architecture for electronic commerce over open networks such as the Internet. The initial *SEMPER* architecture is described in deliverable D03 (“Basic Services, Architecture and Design”). The architecture of *SEMPER* is open: new service modules can be integrated via generic API's, e.g., new payment instruments can be supported by the generic payment API.

The objective of this deliverable are new payment systems. The focus is on the most frequently used payment model on the Internet. This is the direct and account-based payment model, which includes credit-card payment systems and electronic cheques (e-cheque).

For credit-card payments there is the de-facto standard Secure Electronic Transaction (SET) protocol. SET is not in commercial use today, but it is expected to become a dominant protocol within the next years. SET specifies a software-only payment system as a multi-party protocol based on a global Public Key Infrastructure (PKI). There is a clear trend to secure user devices, e.g., smart cards, as already supported by the SET variants C-SET (Chip-SET) and e-COMM. General support for smart cards is expected to be specified in the next version of SET.

For e-cheque payment systems no (de-facto) standard is currently available and different systems have been proposed. The most promising systems are the Electronic Check of FSTC (Financial Services Technology Consortium) and MANDATE II (Managing and Administrating Negotiable Documents And Trading them Electronically), which is funded under ETS, INFOSEC. Both are based on a PKI and secure user devices as already proposed for credit-card payments. For Europe, MANDATE II is preferable to FSTC. Moreover, MANDATE II supports loss tolerance.

This deliverable includes the specifications for the integration of e-cheques in *SEMPER*. As the next step, a prototype integration of MANDATE II in *SEMPER* is considered according to the outlined specifications. This will be achieved in close cooperation with the MANDATE II project.

TABLE OF CONTENTS

FIGURES

TABLES

1 Introduction

The growing activity of business over the Internet increases the demand for an open global framework for Electronic Commerce (EC) [COM97], [ECOMM] with secure payment systems. The main electronic payment methods for EC are modelled after the paper world, such as electronic cash [Ch82], electronic cheques [L82] and electronic credit-card payments [SET97].

This report focuses on electronic cheques and credit-card payments, which can be characterised as direct account-based payment systems [AASW98]. An overview of operational and new payment instruments is given with special attention to the security. Public Key Infrastructures (PKI) and secure user devices are recognised as central security elements for new payment instruments.

SEMPER provides an open architecture for the payment block that allows to incorporate new external payment systems. An important aspect of this report is the extension of the SEMPER payment block for e-cheques. These extensions are described and specified.

This deliverable is structured as follows. After this introductory section, Section 2 describes two direct account-based payment systems, the electronic credit-card and the electronic cheque systems. In Section 3, an overview of the relevant existing or planned electronic cheque systems is given. Section 4 contains the specifications of the new classes in the SEMPER payment block for the integration of electronic cheques. Section 5 describes the hardware-based payment systems MANDATE II [Mandate] for e-cheques as well as e-COMM and C-SET, which are based on SET. In Section 6, the conclusions and an outlook are given. The Annex contains a glossary and an URL to the JAVADOC of the e-cheque interface.

2 Direct Account-Based Payment Systems

2.1 Overview

Payment systems and commerce are moving from the traditional world to the Internet. With this move payment systems become more abstract: payer and payee no longer meet face-to-face, value (i.e., 'money') is represented by electronic data and communication takes place over the open and insecure Internet. This raises security concerns about the authenticity of the various players as well as the integrity and confidentiality of messages.

The new payment systems over the Internet have their counterparts in the conventional world. Payment systems on the Internet exist for electronic cash, cheques and credit-cards. They typically involve four players: the payer, the payee, the issuer (payer's financial institution) and the acquirer (payee's financial institution).

The payment systems used most often on the Internet are characterised as direct and account-based [AASW98]. ‘Direct’ points to the direct communication between the payer and the payee. ‘Account-based’ is related to bank accounts: the payer has an account to be debited for a payment, the payee has an account to be credited after payment. The direct account-based systems include credit-card (see Section 2.2) and electronic cheque payments (e-cheques, see Section 2.3).

Figure 1 depicts the message flow between the players in a direct account-based payment system. In step 1 the payer gets a permission from his bank for the use of e-cheques or credit-card payments, which can be in form of an electronic chequebook, credit-card or in form of certificates. After this initial step the payer can pay different payees for many purchases (step 2). The payee can deposit the received e-cheque or electronic payment slip (step 3). The actual money transfer from the payer's bank account to the payee's bank account occurs between the financial institutions (step 4).

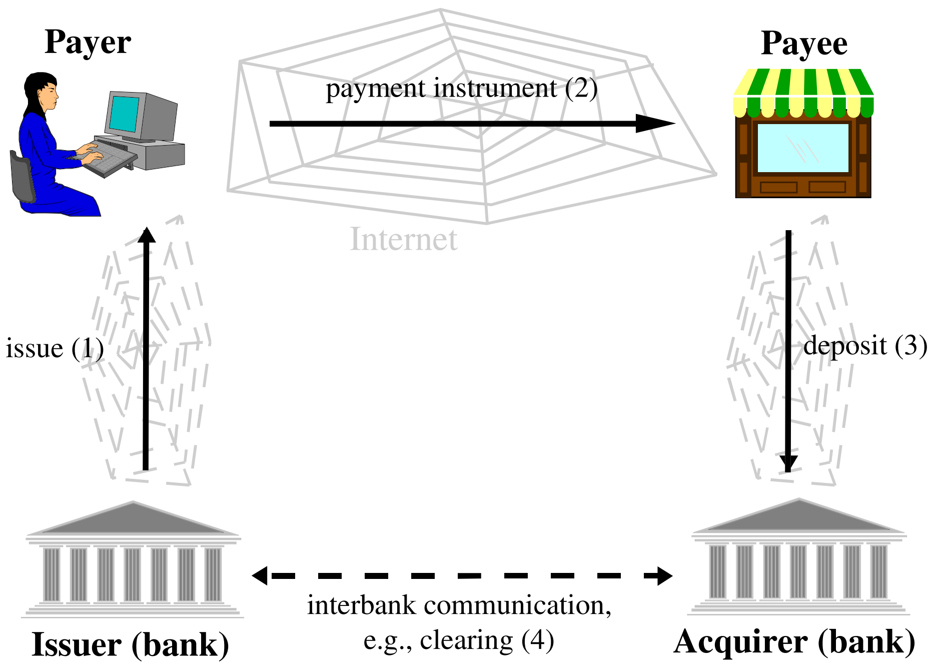

Figure 1: Message flow of direct account-based payment systems.

In direct payment systems the payer always communicates with the payee over the Internet. We only consider the communication for issue, payment and deposit. The interbank clearing, the notifications of the users that the money transfer took place, and the connection of the banking network to the Internet via a payment gateway [D14] are outside the scope of this report.

Communication for offering and ordering of goods as well as delivery is typically outside the scope of a payment system [D03]. The payment system may include a link or hash value of the ordered goods. A payment system does not imply the purchase of goods at all: it just transfers value from the payer to the payee.

2.2 Operational Credit-Card Payment Systems and SET

This chapter gives a short overview on operational credit-card payment systems and focuses afterwards on Secure Electronic Transaction (SET). This chapter provides a suitable framework for the sections on C-SET (Section 5.1.1) and e-COMM (Section 5.1.2) .

2.2.1 Operational Credit-Card Payment Systems

The process of using credit-card payments over the Internet is similar to the process of using the credit-card in conventional sales transactions: there is a purchase request and response between the buyer (payer) and merchant (payee) and there is an authorisation and a capture request-response pair between the merchant and acquirer. Credit-card payments over the Internet may involve additional participants, e.g., a payment gateway (see Section 2.2.2) when using the SET protocol.

There are several credit-card payment systems in operation today:

- The simplest method of credit-card payments over the Internet uses plain text without any cryptographic procedures ('just-do-it'). This payment method does not provide any security. Usually a Web form requests the payment data from the buyer. These data includes the card number and expiration date. The data is sent directly to the merchant.
- Credit-card payments most often take advantage of SSL (Secure Socket Layer) [SSL], which creates a secure channel over the Internet. SSL provides authentication of the server, data encryption and message integrity. With a Web form the credit-card number and expiration date are requested from the buyer and the data is transmitted to the merchant taking advantage of encryption (typically 40 bit encryption only).

  Authentication of the buyer and non-repudiation are not ensured. The communication over the Internet is limited to the transfer of data between buyer and merchant; the acquiring bank does not communicate over the Internet (no multi-party protocol).

2.2.2 SET

Secure Electronic Transaction (SET) [SET97] specifies a technical protocol for securing credit-card transactions over the Internet using cryptography and a public key infrastructure. SET was developed by Visa and MasterCard, with participation from several technology companies, including Microsoft, IBM, Netscape, SAIC, GTE, Terisa Systems and Verisign. SET is still in the experimental phase. Commercial use of SET is expected to start at the end of this year.

SET describes a multi-party protocol that establishes a link between the buyer, merchant and the payment gateway of the acquiring bank. The payment gateway connects the Internet to the existing traditional payment infrastructure. The gateway will either be run by the acquiring bank or by a company contracted by the acquiring bank to do so on their behalf.

Protocol flow:

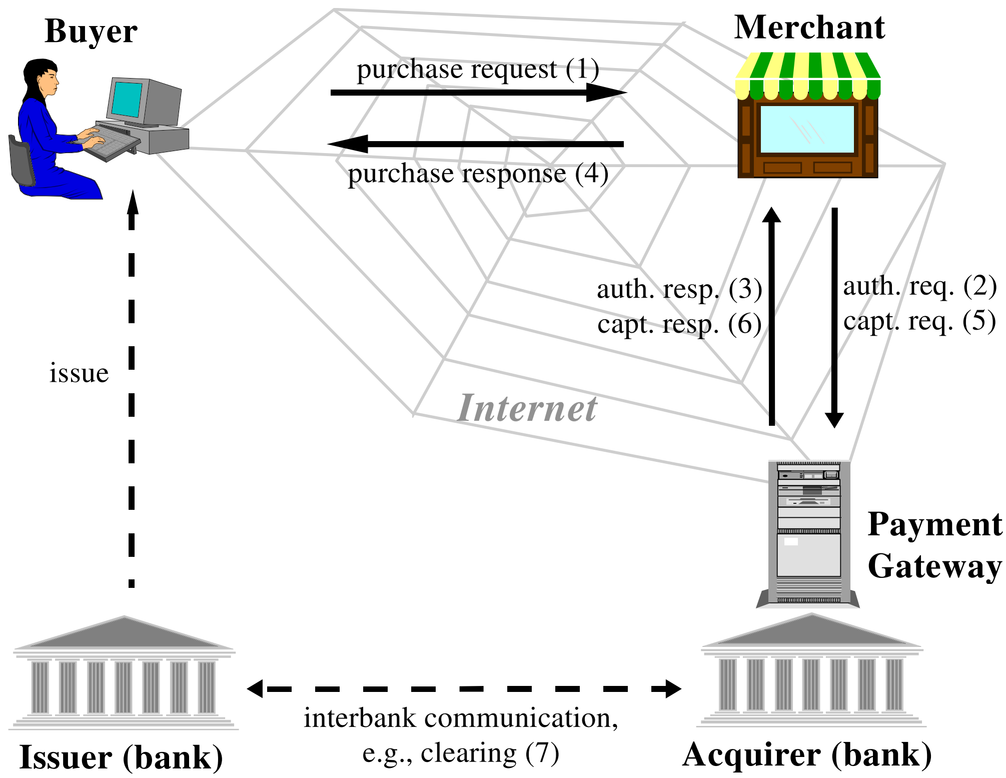

Figure 2: Message flow of SET.

At the beginning, the buyer registers with his credit-card organisation to get a certificate issued by his bank (certificates for the cardholder are optional in a first phase of SET, thus this step may not be required). This has to be done only once before the buyer can run many payment transactions over the Internet. Such a payment typically consists of the following steps (see also Figure 2):

1. The buyer has decided what he wishes to shop, where to ship etc. The buyer clicks the 'Pay' button in his Web application, chooses the credit-card to use, and clicks 'OK' to forward the purchase order with encrypted payment information (including the credit-card number) to the merchant. The purchase order is digitally signed.
2. The merchant sends an authorisation request to the payment gateway. The payment gateway is under control of the acquiring bank. The authorisation request includes encrypted data digitally signed by the merchant and 'tunnelled' data from the buyer (encrypted and digitally signed by the buyer). The merchant cannot see the buyer's credit-card information.
3. The payment gateway returns to the merchant an authorisation response (which may have been requested by the acquirer from the issuer over the regular financial network, not in the scope of SET). The authorisation means payment guarantee to the merchant.
4. The merchant returns a purchase response to the buyer. This completes the purchase from the buyer's point of view.
5. The merchant requests actual payment by sending a capture request to the acquirer.
6. The capture response is returned from the acquirer to the merchant. The purchase is now complete from the merchant 's point of view.

7. The remaining transactions such as interbank clearing and settlement are not in the scope of SET.

SET transactions are actually more complicated than described above, because they include additional sub-protocols for certificate handling and verification. Certificates are used for the buyer (optional in first phase), merchant and payment gateway.

SET provides confidentiality by encryption, strong authentication of buyer (optional in first phase), merchant and acquirer (i.e., payment gateway). The use of buyer's certificates support non-repudiation of payments. In a later version of SET, secure user devices are planned.

2.3 E-Cheque Systems

E-cheque systems will be described by a top-down approach. First we give a generic definition of e-cheques without referring to a specific design and then compare it to credit-card payments (Subsection 2.3.2). In Subsection 2.3.3, we present the typical life cycle of a cheque. The following subsection contains the basic e-cheque structure and the basic message flow (the specific design of the extensions of the SEMPER payment block for e-cheque systems is given in Section 4). In the last subsection, basic security issues are presented.

2.3.1 Definition

An electronic cheque (e-cheque) is a direct account-based payment instrument (see Section 2.1 and Figure 1). Each e-cheque is uniquely numbered. Banks may control the number of e-cheques that are issued within a limited period of time. An e-cheque system can have the following optional features:

- The amount paid with an e-cheque may be guaranteed by the issuing bank.
- An e-cheque can be endorsed.

2.3.2 Comparison with Credit-Card Payments

Credit-card payments differ from e-cheques by the presence of a credit-card company. A credit-card payment can only be accepted by merchants, who have a signed contract with an acquiring bank licensed by the same credit-card company. A credit-card payment is an open payment instruction from the buyer to his issuing bank in favour of the merchant. Unlike an e-cheque, credit-card payments cannot be endorsed.

2.3.3 The Typical Life Cycle of Cheques

Typically, the paper cheque passes through the following life cycle. Cheques are issued by the issuing bank and sent to the customer in form of a chequebook. The unforgeably structured surface on the cheques testifies that the cheques are genuine and provides uniqueness. The bank account information that is given on the cheque makes an implicit statement that the payer is the owner of this account and that the bank will pay the payee from this account. When a payer writes (or draws) a cheque he confirms it by his signature (after filling in the amount) and presents it to the payee. The drawn cheque is a security, which gives its owner the right to deposit the cheque at an acquiring bank and to obtain the specified amount in return [GA31]. As an option, the cheque can be endorsed to an other payee, i.e., a cheque can be passed on by the payee to some other person/business who in turn will be able to deposit the cheque or pass it on further. In this way, a chain of successive payers and payees is obtained. This property of cheques will be referred to as endorsability.

An e-cheque mirrors the paper cheque and provides the following authenticated statements at the different stages of its life cycle (see Figure 1).

- **Blank e-cheque**: A blank e-cheque in the chequebook of the payer contains a serial number and information on the payer's bank account. This information is authenticated by the issuing bank for example by a valid payer-certificate.
- **Drawn e-cheque**: The payer draws the e-cheque in favour of the payee and signs it beforehand. The e-cheque must contain date and time, the proper amount to pay. It can contain further information such as the payee's name and address, and possibly optional information about purchased goods. By signing the e-cheque the payer commits himself to the stated amount.
- **Deposited e-cheque**: When depositing the e-cheque, the payee adds date and time as well as information about her bank account to which the amount should be transferred. This information has to be authenticated for instance by a digital signature of the payee.
- **Endorsed e-cheque:** Instead of directly depositing the e-cheque (at the acquiring bank), the payee can pass on the cheque to another party in exchange of the stated amount using a similar protocol.

A fully completed e-cheque, must contain all information necessary to invoke the actual money transfer from the payer's to the payee's account.

2.3.4 E-Cheque Structure and Message Flow

To mimic the paper cheque, the e-cheque must contain the following minimal information:

1. serial number, which is a unique identifier for the cheque
2. issuing bank identifier
3. account information of payer (e.g. a unique fingerprint of the payer's account number)
4. amount to be paid and currency
5. date and time of completion of cheque.

Additionally, an e-cheque will contain deposit/endorsement information and possibly guarantees for authenticity of signatures (e.g. certificates). The actual structure depends on the specific design of a particular e-cheque system. In the current design (cf. Section 4.2.1), the generic class *Cheque* contains the attributes mentioned above. Further attributes can be specified in an extension of the class *Cheque*, e.g.,

- certificate of payer's bank
- certificate of first payer
- signature of first payer
- account information of (ultimate) payee

- date and time of ultimate/intermediate cheque endorsements(s)
- signature(s) of ultimate/intermediate payee(s)
- certificate(s) of ultimate/intermediate payee(s)
- information about purchased goods or invoice information.

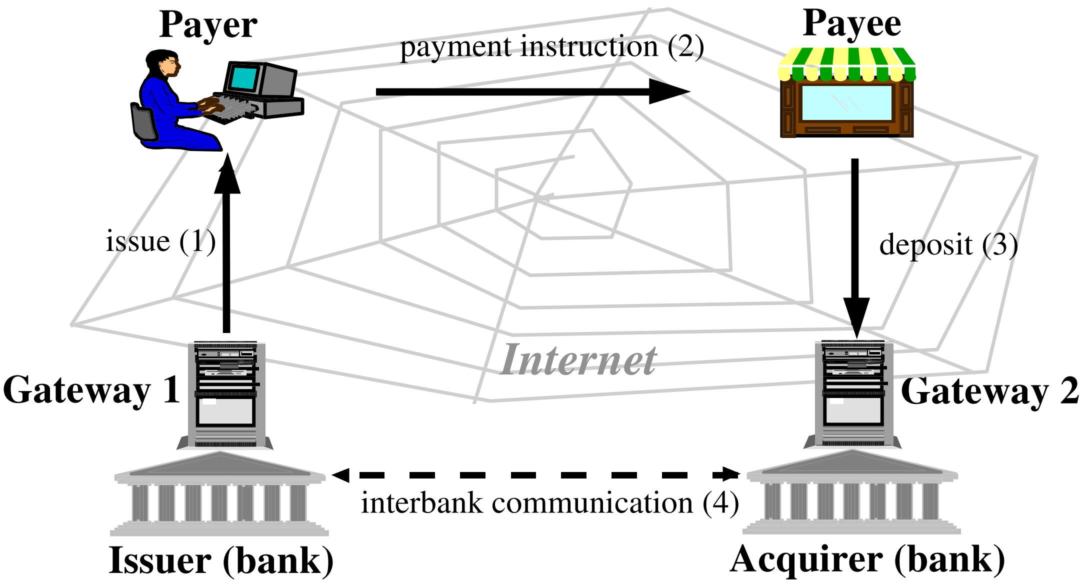

Figure 3: Basic message flow of an e-cheque system.

The message flow that is modelled after the paper cheque system is shown in Figure 3 where for the sake of simplicity just one payer and one payee (and no intermediate payees) are included. Steps 1 to 3, correspond to the blank, the drawn and the deposited e-cheque in the life cycle of a cheque. Step 4 makes use of the interbank communication for clearing and settlement (which is not within the scope of this deliverable). When the e-cheque is endorsed to an other party, the payment at Step 2 is made to an intermediate payee (or chain of intermediate payees) before the cheque is eventually deposited (Step 3).

2.3.5 Basic Security Issues

The security of an e-cheque depends on technical but also banking procedures, like banking policies. In this report, separate generic security issues will be considered, which can be used to assess different e-cheque systems. The following issues are of particular importance.

- **Trust relations:** There are different trust relations, which will be referred to as symmetrical and asymmetrical relations, between the various players of an e-cheque system depending whether there is equal mutual trust or not between the players.

  The most solid trust relation persists between the payer’s and the payee’s bank. In general, both banks are large and well-established institutions and their business relation is regulated by national and international law. Their relation can be viewed as a symmetrical trust relationship.

The relationship between the payer and his bank is an asymmetrical relation. In general, the payer is supposed to trust in his bank. The bank, however, will not trust in the payer in the same way. The trust of the bank may depend on how the payer guarantees to cover his account. To avoid the critical trust relation “trust of the bank in its customer”, any higher risks have to be excluded by the technical and organisational concept of the e-cheque payment system itself. No bank will use any system where it is forced to put too much trust in the customers.

The relation between the payee and the bank is similar to the one of the payer and his bank; it is an asymmetrical relation. For e-cheques, the important relation is the trust of the payee in her bank (and the customers are supposed to trust in their bank).

In most cases, there is no direct trust relation between the payer and the payee. However, the three previous trust relations provide an indirect trust relation from the payee in the payer or, more precisely, in the cheque of the payer. The critical part in the indirect path of trust is the relation between the payer and his bank. This weakest link in the trust chain can be reinforced in several ways. One way consists in an enhanced liability of the payer, which is reflected in the terms and conditions of the issuer. E.g., a chequebook of e-cheques with bank guarantee would be only delivered if the account holder had a sufficient positive balance of which some part is reserved to cover incoming deposited e-cheques. Another way would be to use a voucher or a prepaid cheque.

- **Issuing policy:** The way that e-cheques are handled and charged on a payer’s account is critical for their security, from the bank’s point of view. The terms and conditions between payer and issuing bank determine how many cheques can be issued within a limited period of time and up to which guaranteed amount.
- **Guaranteed amount:** It is crucial for the recipient of an e-cheque (usually the merchant) to know up to which amount the value of the e-cheque is guaranteed by the bank. Similarly to the paper world, this will determine the willingness of the recipient to accept a cheque or not.
- **On-line and off-line systems:** The usual way to enhance the security of the payee is by using on-line payment systems [AJSW97]. Aided by an on-line request, the payee can verify that an e-cheque is covered. Moreover, the payee will get an authorisation notice in return to his request. Such a notification is desirable from the payee’s point of view.
- **Loss tolerance:** Since connections over the Internet are not reliable (nor the player’s machines), the e-cheque system should be loss tolerant, i.e., if an e-cheque is lost during transmission (or during internal processing at the payee or at a bank), this event should not be critical for the further processing of this e-cheque. There are different possible measures to achieve loss tolerance. One way is to store an extra copy in an archive, which allows the holder of the cheque to retrieve it, in case it is lost or was not successfully transmitted. Another way - as done in MANDATE II (cf. Section 5.2) - is to send it to a trusted third party, who will safely store this extra copy and make it available in case of lost.
- **Public key infrastructure:** When digital signatures are used, a public key infrastructure (PKI) is required. The most common way of key distribution makes use of certificates, which are issued by a trusted third party (mostly using the ISO

X.509 certificate standard). To check digital signatures, one uses a copy of the signing party's public key, which must be trusted.

- **Confidentiality:** Sensitive data (e.g. account numbers, amount) should be kept confidential and messages that contain such data should be encrypted or sent over a secure channel.
- **Secure user devices:** The most serious security threats arise if some secret key of a player is compromised. The impact of this threat can be reduced using a PKI (e.g., by checking certificate revocation lists). Other means to prevent the theft of the secret key is the installation and use of tamper-resistant devices. These devices perform the basic cryptographic functions (including the generation of the public/private key pair) required for signing or encryption and prevent that another copy of the secret key is available outside the tamper-resistant device. Additionally, the secret key must be protected at least by a PIN known exclusively to the holder.

  The tamper-resistant user device can be considered to be a bank's agent sitting at the client's computer. Thus, it strengthens the trust relation between the payer and the payer's bank and between the payee and the payee's bank. In this respect, the purpose of the tamper-resistant hardware is to guarantee the uniqueness of each e-cheque that leaves the device.
- **Double spending:** In electronic payment systems, where a value is represented as a sequence of bits, copying is a conceivable system weakness, which can result in double spending of the payer and double depositing of the payee. Mechanisms to prevent these threats must be provided. Possible counter-measures should achieve uniqueness of an e-cheque and rely for instance on on-line payment systems or secure user devices.
- **Anonymity and unlinkability:**

  a) Anonymity of payer towards payee: For some applications there will be payers who would not like their identity being revealed to the payees. This type of anonymity can easily be achieved using pseudonyms for the payer's bank account, name and address without compromising the security of an e-cheque. Additionally, the PKI must support anonymity; e.g., certificates must also contain a pseudonym for the payer. Moreover, it is assumed that the communication channel does not reveal the identity of the sender (the payer).

  b) Unlinkability: In principle, one can also achieve unlinkability of the payer by the payee. This would require e.g. to use a different pseudonym for each payment.

3 Existing and Proposed E-Cheque Systems

An overview on existing or new relevant e-cheque systems is given, as far as known to us at the time of this writing. The e-cheque systems Electronic Check of FSTC, NetCheque and MANDATE II are based on the message flow presented in Section 2.3.4. NetBill, ECheque and PayNow make use of a central server. Other systems like NetChex and Redi-Check [Redi-Check] will not be considered here as they are not direct account-based (i.e., there is no communication between payer and payee, not even through an intermediate server). Each of the following subsections describes one of the considered systems independently. For easier comparison of the systems, a set of characteristic requirements and security criteria has been chosen. A table for each system shows which of them are fulfilled. Additionally, all tables are comprehended in Table **7**, Section 3.7.

3.1 The FSTC Electronic Check

3.1.1 Overview

The Electronic Check project [FSTC] of the Financial Services Technology Consortium (FSTC) developed a model for electronic cheques and implemented a prototype. The detailed design is not publicly available but the basic structure of an FSTC e-cheque is likely to be based on the proposed structure described in Section 2.3.4. To extend the functionality of the e-cheque system the design allows to integrate it conveniently with electronic ordering and billing systems.

The proposed e-cheque model goes beyond conventional paper chequeing and provides security features common to electronic cheques such as digital signatures of all involved parties and encryption of exchanged e-cheques. In particular, a mechanism is designed into the Electronic Check to prevent interception and fraudulent use of account numbers by eavesdroppers. The security is achieved using public key cryptography.

Electronic Checks can be endorsed. Moreover, an e-cheque can be split into ‘smaller’ e-cheques whose individual amounts sum up to the initial total amount. (This splitting feature is not realistic from the European bank’s point of view.)

Moreover, additional new services are proposed using three other message flows than those shown in Figure 3. These new services - different from the one of Figure 3 - will not be considered as e-cheque systems since the definition of Section 2.3.1 does not apply.

3.1.2 Secure User Devices

Public key cryptography as used in this project will require a public key infrastructure, which supports certificates. Moreover, the secret keys used for signing and encryption must be stored safely in a tamper-resistant device. FSTC proposes different solutions for the implementation of tamper-resistant devices [FSTC]. A key innovation is the use of an Electronic Checkbook to generate e-cheques. Three alternatives for the implementation of the Electronic Checkbook are proposed:

1. Tamper-resistant PCMCIA card. The card contains a mechanism to generate or store unique cheque identifiers, to maintain a cheque register, and to calculate and verify digital signatures and certificates.
2. Smart card. The Electronic Checkbook (or possibly a reduced version due to memory limitations) is implemented in an ISO format for smart cards.
3. Cryptographic hardware processors. Secure hardware processors are attractive for processing large volumes of cheques or for storing a number of Electronic Checkbooks.

3.1.3 Modularity and Open Interfaces

The high level services include management functions for issuing, cheque writing and cheque depositing. These services make use of basic modules providing, for instance, cryptographic services such as the generation and verification of digital signatures on e-cheques. Moreover, when using hardware devices that contain the Electronic Checkbook suitable interfaces will perform the interaction with the core application. This modularity and the use of standard interfaces is of particular interest to SEMPER.

Criterion	Match
Central server required	
On-line connection required (to central server)	
Certificate infrastructure required	✓
Secure hardware	✓
Number of banks	multiple (any bank)
Operational	(Prototype)
Loss tolerance	
Endorsability	✓
Confidentiality (using strong/weak cryptography)	✓ (strength unknown)
Non-repudiation (payer/payee)	both
Message integrity	✓

Table 1: Overview of the FSTC Electronic Check.

3.2 NetCheque

The NetCheque payment system is an electronic payment system for the Internet developed at the Information Sciences Institute of the University of Southern California [NM95], [NetCheque]. Users registered with NetCheque accounting servers are able to write electronic cheques to other users. These cheques may be sent through e-mail or as payment for services provided through other network protocols. When deposited, the cheque authorises the transfer of account balances from the account against which the cheque was drawn to the account to which the cheque was deposited. The payment system is designed for micro-payments, such as pay-per-view pages on the Internet.

In order to use NetCheque the user has to register with NetCheque and open an NetCheque account. Clearing is done through a NetCheque server and means settling balances of NetCheque accounts. Currently, there is no bank support and, thus, there is no real money transfer from the payer's bank account to the payee's bank account.

Instead of using digital signatures (for payer and payee) NetCheques makes use of Kerberos tickets, which are generated by a central server. The Kerberos tickets provide authentication of the players (payer and payee) towards the accounting server of the payer and are considered as 'signatures' by the designers of NetCheque [NM95][NetCheque]. (Note that the Kerberos authentication is based on conventional cryptography, therefore, no true digital signature is obtained and non-repudiation is not supported.)

A NetCheque contains the following information:

1) Amount

2) Currency

3) Expiration date

4) Account information

5) Name of payee

6) 'Signatures' and 'endorsements' accumulated during processing.

1) - 5) are readable by bearer. The 'signatures' and 'endorsements' are verifiable by the accounting server against which the cheque was drawn.

3.2.1 Issuing

The information described in 1) - 5) is entered by the payer. A Kerberos ticket is obtained; this will be used to authenticate the user to the accounting server. The user generates an authenticator with an embedded checksum, and places the Kerberos ticket and the authenticator in the 'signature' field.

The cheque is base64 encoded and can be sent through e-mail.

3.2.2 Depositing

The payee obtains a Kerberos ticket to be used with the payer's accounting server, generates an authenticator containing the payee's account information and appends this (the so-called 'endorsement') to the cheque. An encrypted connection is opened to the payee's accounting server and the endorsed cheque is deposited.

As the NetCheque is cleared through multiple accounting servers (in the case that payer and payee have their NetCheque accounts on different servers), each server attaches its own 'endorsement', similar to the 'endorsement' attached by the payee.

Criterion	Match
Central server required (its purpose)	✓ (authentication)
On-line connection required (to central server)	✓
Certificate infrastructure required	
Secure hardware	
Number of banks	multiple account servers (no banks)

Operational	✓
Loss tolerance	
Endorsability	
Confidentiality (using strong/weak cryptography)	
Non-repudiation (payer/payee)	
Message integrity	✓

Table 2: Overview of NetCheque.

3.3 PayNow from CyberCash

PayNow™ is a recently developed e-cheque system from the security company CyberCash in Reston, Virginia, USA [PayNow], [S97], [rfc1898]. In the beginning of February 1997, CyberCash has started a pilot program for secure electronic cheque service together with companies like Kansas City Power & Light, Princeton TeleCom Corp. and Cephas Multimedia Inc.

To the client (payer), the e-cheque system PayNow looks similar to conventional paper chequeing. To use this system, the client must first create a (software) wallet, which contains information about his or her checking account located at some issuing bank. The e-cheque application PayNow uses this account information for subsequent payment transactions. An e-cheque is presented on the screen in a similar way as a paper cheque, i.e., it contains the payer's address, bank account information and the amount. Cheque writing in this manner (and deposited by the payee) will appear on a monthly checking account statement in the same way as paper cheques.

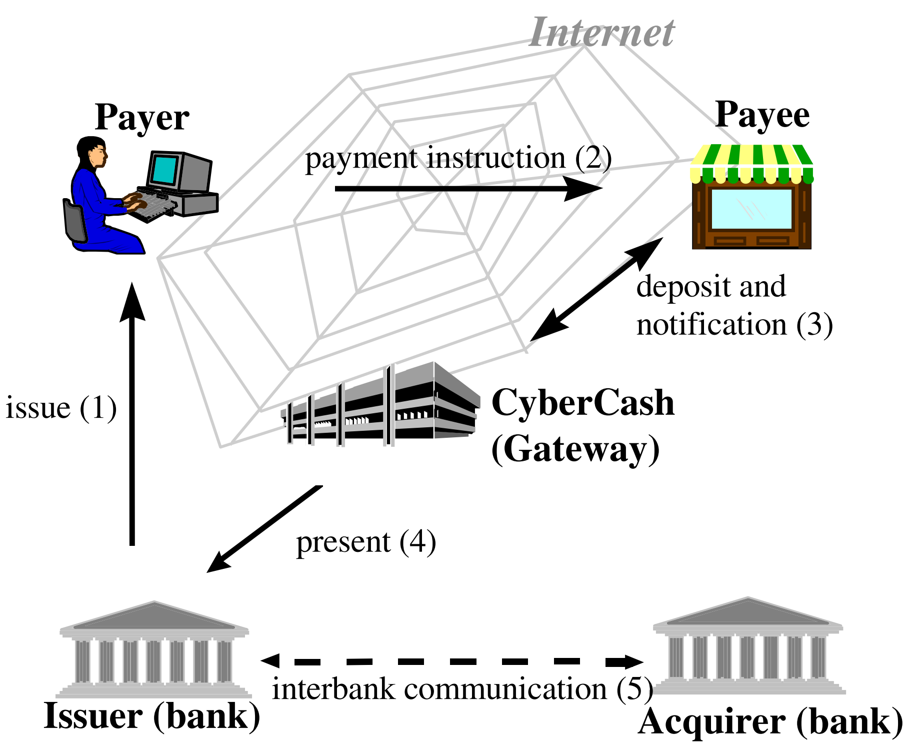

Figure 4: Message Flow in PayNow.

The message flow in the CyberCash system PayNow is shown in Figure 4. This e-cheque system differs from the proposed system in Section 2.3.4 in the sense that there is an intermediate player, viz., the CyberCash Gateway, which is crucially involved in the e-cheque protocol. The gateway has stored the public keys of all other players and, thus, is able to check signatures of the payer and the payee. Upon receipt of an e-cheque, the payee does not check the payer’s signature but transfers the cheque to the gateway, where the signatures are checked. The gateway notifies the payee about the validity of the cheque and, eventually, presents the e-cheque (or a batch containing many e-cheques from previous transactions) to the issuing bank of the payer.

In the CyberCash model, the installation of the Public Key Infrastructure (PKI) is rather simple and no certificate chains are required. In the initialisation phase, a user is in possession of the public key of the gateway, which is incorporated in the user software. In a first step, each user has to go through a registration process, where he presents some credentials to the registration authority. On the technical side, the user generates an RSA key pair and then sends his public key to the gateway in encrypted form. The gateway stores all user identifications together with their public keys. Thus, the gateway is able to verify all signatures. Moreover, if a secret key of some user is compromised, then the gateway can cancel the corresponding public key and ask the user to create a new key pair (It is not clear whether this mechanism is implemented in the pilot). The only critical issue in this PKI is the distribution of the public key of the gateway. In case that the secret key of the gateway is compromised the system’s security will break down and there seems to be no mechanism to replace a compromised secret/public key pair of the gateway. The merit of this centralised PKI is that no external hierarchical certificate infrastructure is needed. The reverse side of the central server is that it can become a bottleneck; hence, it must meet very high reliability and availability standards.

The (opaque part [rfc1898] of the) exchanged messages between payer and payee and between payee and the gateway are encrypted using symmetrical encryption and random session keys, which in turn are encrypted using the public key of the gateway or the payee’s public key. The encryption relies on industrial strength 768-bit RSA and 40-bit DES. (Note that at the current stage of cryptanalysis, the 40-bit key DES encryption is not considered to be secure.)

The current software, which is used in the pilot, can be downloaded for free from the CyberCash server at the Internet address ‘ftp.cybercash.com’. The system does not make use of tamper-resistant hardware but consists of software only. This software is also used to encrypt the user’s account data on his local machine. This application program is vulnerable to Trojan horse attacks, which steal the user’s password. Such an attack might result in getting complete access to the user’s account data as well as to getting full control over the user’s wallet.

Criterion	Match
Central server required	✓
On-line connection required (to central server)	✓
Certificate infrastructure required	

Secure hardware	
Number of banks	multiple (any banks)
Operational	✓
Loss tolerance	✓
Endorsability	
Confidentiality (using strong/weak cryptography)	weak
Non-repudiation (payer/payee)	✓
Message integrity	✓

Table 3: Overview of PayNow.

3.4 ECheque

The e-cheque system 'ECheque' was developed by MarketNet, which is an Internet service provider [ECheque]. Together with Secure Trust Bank plc. MarketNet has founded BankNet, which provides on-line banking services. ECheque is an electronic cheque service. To use this service either as a customer or as a merchant, it is necessary to have an account with BankNet. Thus, the ECheque service is restricted to writing e-cheques only to other clients of BankNet. MarketNet plans to broaden the number of clearing banks such that people banking at clearing banks other than the BankNet branch will be able to deposit BankNet electronic cheques.

ECheque produces digitally signed cheques using public key cryptography. Currently, there is a beta test version of the cheque writing program. It is linked to HTML, but only available for Windows 3.1.

Before a user can write an e-cheque he or she has to do the following.

- Register with MarketNet and open an account at BankNet. For this operation credentials such as a copy of the passport or other identification information is required.
- Generate a private/public key pair and register the public key at MarketNet. The scope of the key, which is given by restrictions such as limited life or limited turnover, can be chosen by the user.

The message flow in the ECheque system is not clear from [ECheque]. It seems that the payer sends the written cheque, containing appropriate payee information, to the central MarketNet server and no direct communication between payer and payee takes place except for messages that are exchanged via the Internet browser or email. MarketNet in turn hands the e-cheque directly to BankNet (the only bank in this system) for clearance. It is not mentioned whether the payee signs the written cheque before it is deposited.

The connection between a user and MarketNet is protected by encryption using either the Secure Socket Layer (SSL) software or 'WorkHorse', which is a specially developed SW from MarketNet. Since the ECheque system uses a central server no certificate infrastructure is required.

The ECheque system is a pure SW solution and does not make use of tamper-resistant hardware and, thus, it is vulnerable to Trojan horses.

Criterion	Match
Central server required	✓
On-line connection required (to central server)	✓
Certificate infrastructure required	
Secure hardware	
Number of banks	only one issuing bank
Operational	✓
Loss tolerance	
Endorsability	
Confidentiality (using strong/weak cryptography)	weak
Non-repudiation (payer/payee)	✓
Message integrity	✓

Table 4: Overview of MarketNet.

3.5 NetBill

NetBill is a research project at Carnegie Mellon University in conjunction with Mellon Bank and CyberCash [NetBill], [ST95]. In the NetBill model a payer, represented by a client computer, wishes to buy information from the payee's server. A NetBill server maintains accounts for both consumers and merchants. These accounts are linked to conventional financial institutions.

Although NetBill uses an electronic chequebook library at the payer’s side, it does not fit exactly in the electronic cheque model described in Section 2.3.4. One (minor) difference is that both payer and payee need to have accounts at the same place. Hence the Issuing Bank and the Acquiring Bank in Figure 3 are replaced by one entity namely NetBill. Another difference is that the NetBill is a goods-for-money exchange system that involves the NetBill server in each transaction. The system is not intended to be used as a payment instrument without immediate exchange for goods, but rather for payments due to an invoice.

When a payer creates a NetBill account, he receives a unique user ID and generates the RSA public key pair associated with that ID. This key pair is certified by NetBill, and is used for signatures and authentication within the system. NetBill does not make use of secure hardware and, thus, it is vulnerable to Trojan horse attacks.

Before a payment is made, the payer sends a digitally signed *purchase request* to the payee. The payee computes a checksum, and sends the encrypted goods with a time stamp to the payer. The payer's software computes a checksum of the encrypted goods, and sends this, along with the accepted price, the product identifier, and the time stamp back to the payee. This information is collectively called the *electronic* *payment order*, or EPO. At this point, the payer has the goods but cannot decrypt them, and no payment has been made.

When the payee receives the EPO, the payee's server compares the two checksums and, if they do not match, retransmits the data or aborts the operation. This step ensures that the encrypted goods were transmitted without error.

Once the encrypted goods have been received and verified, the payee server appends the decryption key to the EPO and then endorses it with the payee's digital signature. The payee then sends this to the NetBill server.

The NetBill server verifies that the product identifiers, prices and checksums are all in agreement. If the payer has the necessary funds or credit in his account, the NetBill server debits the payer's account and credits the payee's account, logs the transaction, and saves a copy of the decryption key. The NetBill server then returns to the payee a digitally signed message containing an approval, or an error code indicating why the transaction failed. The payee forwards the NetBill server's reply and (if appropriate) the decryption key to the payer.

The NetBill server operates transactionally to ensure that the payer does not get billed for goods he cannot decrypt or receive goods without paying for them. If for any reason the transaction can not be completed, NetBill guarantees that the payer will not be charged.

NetBill also uses Kerberos tickets. The NetBill transaction protocol involves several phases, for price negotiation, goods delivery, and payment; only the last of these phases requires non-repudiable signatures using public key cryptography. Instead of using public key cryptography for message authentication and encryption throughout the NetBill system, symmetric cryptography (DES) is used because for performance. The 56 bit key of DES has been successfully attacked, using a network of computers; thus, it should not be considered a cryptographically strong algorithm anymore.

Criterion	Match
Central server required	✓
On-line connection required (to central server)	✓
Certificate infrastructure required	no external PKI (a PKI is provided by NetBill)
Secure hardware	not at payer or payee
Number of banks	multiple (any bank)
Operational	✓
Loss tolerance	✓
Endorsability	
Confidentiality (using strong/weak cryptography)	✓ (DES)
Non-repudiation (payer/payee)	✓

Message integrity	✓

Table 5: Overview of NetBill.

3.6 MANDATE II

MANDATE II (Managing and Administrating Negotiable Documents And Trading them Electronically) [Mandate] is a project under the EC DGXIII ETS (Electronic Trusted Services) programme currently developing an electronic cheque. Central to the technical solution is a 'DOC-carrier' (DC), which is tamper-resistant and implemented in some special hardware such as an advanced smart card. To support loss tolerance MANDATE II makes use of trusted third parties (TTP), which obtain a copy of each drawn e-cheque. Note that these TTPs are not needed to run the cheque system. Since in this report, MANDATE II is considered as a hardware-based payment system, the detailed description is given in Section 5.2.

Criterion	Match
Central server required	no, but one or more TTPs for loss tolerance
On-line connection required (to central server)	
Certificate infrastructure required	✓
Secure hardware	✓
Number of banks	multiple (any bank)
Operational	
Loss tolerance	✓
Endorsability	✓
Confidentiality (using strong/weak cryptography)	✓ (strong)
Non-repudiation (payer/payee)	✓
Message integrity	✓

Table 6: Overview of MANDATE II.

3.7 Summary

The considered e-cheque systems are summarised in Table **7** given below using the same criteria as in the previous subsections. Table **7** can be used to compare the e-cheque systems based on their infrastructure requirements and on the security they provide. New payment instruments (FSTC and MANDATE II) tend to take advantage of a PKI and secure user devices. This Table is intended as an overview. For the details, the reader is referred to the previous subsections.

Criterion	FSTC	NetCheque	PayNow	ECheque	NetBill	MANDATE II
Central server required		✓ (authentication)	✓	✓	✓	no, but one or more TTPs for loss tolerance
On-line connection required (to central server)		✓	✓	✓	✓	
Certificate infrastructure required	✓				no external PKI (a PKI is provided by NetBill)	✓
Secure hardware	✓				not at payer or payee	✓
Number of banks	multiple (any bank)	multiple account servers (no banks)	multiple (any banks)	only one issuing bank	multiple (any bank)	multiple (any bank)
Operational	(Prototype)	✓	✓	✓	✓	
Loss tolerance			✓		✓	✓
Endorsability	✓					✓
Confidentiality (using strong/weak cryptography)	✓ (strength unknown)		weak	weak	✓ (DES)	✓ (strong)
Non-repudiation (payer/payee)	both		✓	✓	✓	✓
Message integrity	✓	✓	✓	✓	✓	✓

Table 7: E-cheque System Overview.

4 E-Cheques in the SEMPER Payment Block

4.1 Introduction

In order to use electronic cheques in SEMPER a sub-interface to the more general *AccountBasedPurseServices* has been added along with a cheque-specific extension of *AccountBasedPurse*. The e-cheque systems of Section 3 can all be supported by SEMPER. For each new e-cheque system, this requires an appropriate adapter and a suitable subclass of the generic cheque class.

4.2 Extensions of the Payment Block

In order to use electronic cheques in the Payment Block this has been extended. The cheque interface reflects the SEMPER definition of electronic cheques. Three classes have been added: *Cheque*, *ChequePurse*, and *ChequePurseServices*. Each cheque will be represented by an object of the class *Cheque*. *ChequePurse* extends *AccountBasedPurse* with methods for viewing information on the contents of the purse. *ChequePurseServices* extends *AccountbasedPurseServices* with methods for managing cheques in the purse. The added classes are discussed in greater detail in the following sections.

4.2.1 Class Cheque

Each cheque will be represented by an object of this class. The attributes of the class are those essential of a cheque:

- _serialNumber – ID of the cheque
- _issuingBank – ID of the issuing bank
- _issuingAccount – Number of the corresponding account
- _amount – Amount of the cheque
- _timeOfIssue – Timestamp for issue

The first two attributes uniquely identify the cheque. Information on the issuing bank and corresponding account is necessary for the clearing process. The timestamp indicates time of completion of the cheque. In most cheque systems the cheques are only valid for a certain period of time.

Some cheque systems, like MANDATE, will need more attributes. In these cases an extension of the *Cheque* class is necessary in the specific adapter.

4.2.2 Class ChequePurse

The abstract class *ChequePurse* extends *AccountBasedPurse* with two methods:

- *getNumberOfCheques* - Returns the number of blank (unused) cheques in purse
- *retrieveCheques* - Returns a list of received cheques in purse

In a cheque purse, unlike an *AccountBasedPurse*, there are only a limited number of payment instruments. In that respect the *ChequePurse* is not unlike a *CashLikePurse* having only a limited number of coins. By using *getNumberOfCheques* the payer can check the number of blank cheques left in the purse. Writing a cheque is of course not possible if there are no blank cheques left in the cheque purse.

With a cash-like purse what matters is the total amount in the purse. When dealing with cheques it is not sufficient to know the sum of the amounts of the received cheques. Instead one would like to have information on e.g. issuer and time of issue along with amount and currency. For that purpose it is necessary to have a method *retrieveCheques* to inspect the individual cheques in the purse. In this way it is possible to see e.g. which ones should be cleared, and which ones should be endorsed.

4.2.3 ChequePurseServices

ChequePurseServices extends *AccountBasedPurseServices* with the following methods:

- *loadNewCheques* – Loads new blank cheques into the purse
- *endorseCheque* – Endorses a particular cheque to a third person.

There are two ways of paying by electronic cheque:

- issue a new cheque, i.e. fill in one of the blank cheques in the purse
- endorse a previously received cheque to the payee.

The first (normal) way of paying is of course only possible as long as the payer has blank cheques left in the purse. When the purse, or electronic chequebook, is empty the payer needs to get new cheques using the *loadNewCheques* method. This method has similarities with the *withdraw* method in a cash-like purse. It is important to note, however, that what is loaded into the purse, are not payment instruments (i.e. objects of value) but merely *permissions* to create a certain number of such payment instruments. The *loadNewCheques* method is included in the general cheque interface because it is an essential feature of a cheque system, as defined in Section 2.3.1, that the number of blank cheques is limited. As a consequence, loading of new cheques, one way or the other, has to be done in a cheque system.

When having received a cheque, there are two things that can be done with it:

- deposit in the acquiring bank
- endorse it to a third person.

There are a number of subtleties here. In the paper-world one would choose a specific cheque to endorse, not just any (number of) cheque(s) adding up to the desired amount. In the payment block, however, it is not possible to point to a specific payment instrument in a purse. As a consequence, if any user interaction is needed when endorsing a cheque it has to be taken care of by the adapter. Furthermore a person willing to accept cheques may not be willing to accept endorsed ones, or only from certain people. The payment block does only have very basic negotiation, so acceptance of endorsed cheques has to be handled by the individual adapters based on purse configuration and user preferences. One way to handle this is to have two purses; one for endorsed cheques and one for first hand cheques. Not having a purse for endorsed cheques (or making it pay-only) takes care that only first hand cheques are accepted. Having a real negotiation as part of a payment would of course be a more graceful solution.

5 Hardware-Based Payment Systems

There is a trend towards the use of tamper-resistant devices to provide additional security for new payment instruments. Early implementations of such hardware-based systems are C-SET, e-COMM and MANDATE II, which are described in the following subsections.

The main purpose of tamper-resistant devices is to securely store secret or sensitive information, like a secret key or a root certificate. Moreover, within e-cheque systems secure hardware is a means to prevent double spending and to achieve uniqueness of an electronic cheque.

5.1 C-SET and e-COMM

C-SET [C-SET] and e-COMM [e-COMM] are two credit-card based payment projects that use the SET [Section 2.2.2] protocol. These two projects, formed in France in mid 1996 involve a part of the main French banks and also Eurocard-MasterCard on one side and Visa on the other side. The common particularity of both systems is that they use smart cards for securing the payment transactions. In the first phase, they use the microchip of the 27 millions B0' smart cards[1] already in use in France and in a second phase the future EMV [EMV] international card standard. In addition to the security, the use of smart cards can facilitate portability and makes the payment situation for the buyer very similar to the current conventional payments. The two projects have similar goals: to promote secure electronic commerce on the Internet on the French domestic market and also across borders. Nevertheless the technical solutions differ: e-COMM uses SET from end to end (buyer's PC, merchant's server, payment server) while C-SET uses SET only for cross-border transactions thanks to translation gateways. It should be still noted that both solutions remain in conformity with the 'CB' Group[2] recommendations for secure telepayment in France.

5.1.1 C-SET

C-SET (Chip Secure Electronic Transaction) is based on SET for international transactions, but for transactions within France it adapts its own protocol, namely, the French 'CB'[2] secure telepayment for the Internet. C-SET provides a high level of security by the use of smart cards and secure smart card readers including a PIN pad and a small display. Sensitive software is executed in a secure environment (smart card reader with PIN-pad and display). No secret or private key is held in the

[1] B0' card is in commercial use in France since 1992. B0' uses the DES secret key algorithm. Its storage capacity does not make the storage of SET certificates possible.

[2] Groupement des Cartes Bancaires 'CB' is a joint venture, created in 1984 to implement, coordinate and promote inter-banking of bank cards acceptance in France. It is a private institution, made up of all banks (French or foreign banks) participating in the 'CB' issuing and acceptance system. For information, all 'CB' cards are B0' smart cards and over 90% of transactions are now made with PIN control.

computer of the buyer, nor in the PIN-pad. Only the public key of the payment gateway and a passive authentication value are distributed to buyers and merchants. Transactions are authenticated by a message authentication code computed on the payment data by the card. The PIN - used to identify the cardholder - is not allowed to leave the PIN entry device (smart card reader), and must be presented to the smart card as soon as entered. This protects against Trojan Horse attacks, which otherwise may send an amount different from the one displayed on the card reader screen. It seems that a security flaw remains as the information related to the order content cannot be displayed on the same screen.

Mutual identification of merchants and buyers is provided through the use of certified public keys (certificates are supposed to be similar to SET certificates, but in PKCS#1 format, as X509 certificates do not fit in the smart card memory). Buyer certificates are held in the smart cards, providing buyers mobility: they only need their card to pay wherever they go, provided a C-SET trusted smart card reader is present. The transaction (i.e., payment instructions) is encrypted within the PIN entry device, and can be read neither in the buyer's PC, nor on the network, nor at the merchant's computer. The payment gateway has a secure cryptographic device, with the adequate keys to authenticate the buyer, the merchant, and to verify the authentication code of the card on the payment instructions. The payment gateway signs its response with its private key, and both buyer and merchant can authenticate the gateway and have the insurance of integrity of this response, as they have the public key.

For interoperability there are special 'translation gateways' for the connection to the 'rest of the world': these gateways give C-SET buyers and merchants access to international (and domestic) SET transactions (see Figure 5, Figure 6). In practice, these gateways construct SET messages on behalf of the C-SET users.

The use of the future international EMV standard for smart cards is planned for the second phase of the project.

The C-SET protocol has been defined by the French interbank system 'CB' Group. Cybercard is the name of the pilot currently being set-up with the support of Europay France, Crédit Agricole, Crédit Mutuel, Banques Populaires and La Poste.

It should be noted that C-SET has received the agreement of SCSSI, the French government organisation for information system security. This authority delivers authorisations for the use of cryptography in France.

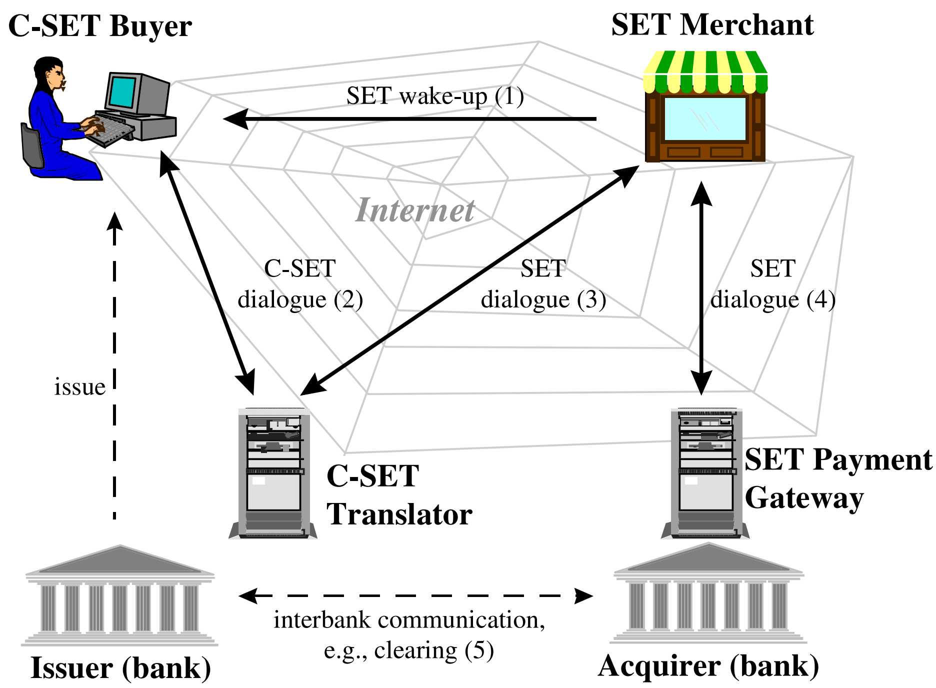

Figure 5: C-SET buyer and SET merchant.

1. SET Wake-up. The buyer recognises the merchant as a SET merchant.
2. C-SET dialogue. The buyer connects to the translator which plays the role of a C-SET merchant for the buyer.
3. SET dialogue. The translator makes the conversion from C-SET to SET and from SET to C-SET. The translator plays the role of a SET buyer for the merchant.
4. SET dialogue
5. Conventional bank network dialogue.

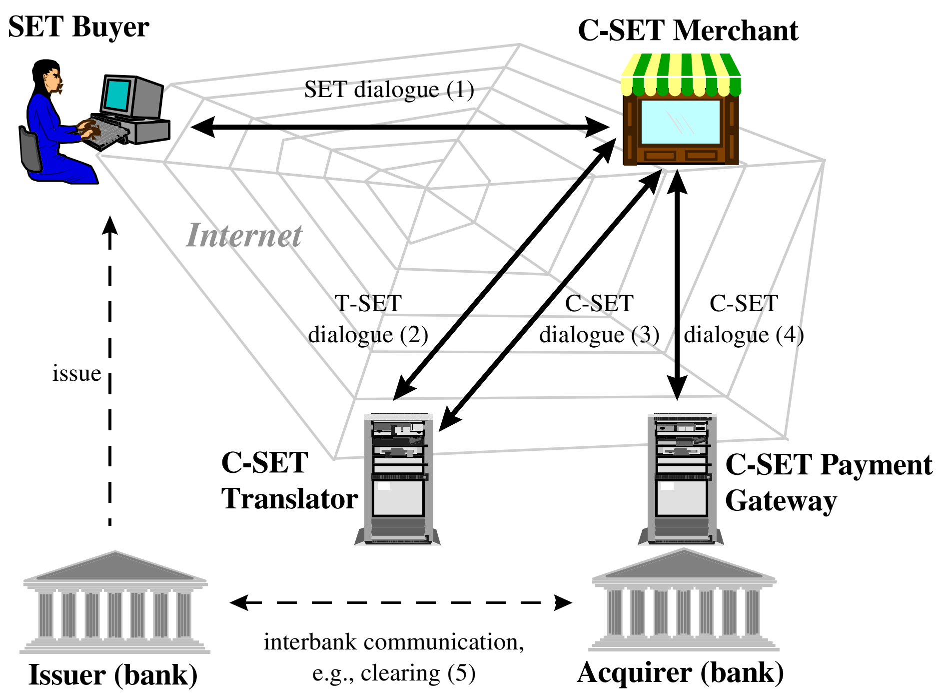

Figure 6: SET buyer and C-SET merchant.

1. SET dialogue. The buyer receives a C-SET wake-up and considers it as a SET wake-up. The buyer starts a SET dialogue with the merchant.
2. T-SET dialogue (stands for Tunnelling SET). The merchant detects that the buyer is a SET buyer. In a specific protocol, the merchant transmits the SET buyer's messages to the translator with additional information about himself.
3. C-SET dialogue. The translator plays the role of a C-SET buyer for the merchant.
4. C-SET dialogue.
5. Conventional bank network dialogue.

5.1.2 E-COMM

The scope of the e-COMM project is similar to C-SET. Additionally e-COMM supports micro-payments. The e-COMM payment system is based on SET for all transactions, also for transactions within France. Like C-SET, e-COMM uses the French 'CB' Group secure telepayment recommendations for the domestic transactions but all the e-COMM messages fit the SET protocol (this is in contrast to C-SET). E-COMM adds to the normal features defined in the SET standard the security given by the 'CB' chip card: local PIN verification by the card, message authentication code of the transaction computed by the card and verified in a secure cryptographic device at the acquirer payment gateway. In case of a foreign merchant and its associated acquirer payment gateway, the protocol is simply the SET protocol.

The use of the future international EMV standard for smart cards is planned for the second phase of the project. For the first phase with B0' smart cards the SET certificate is located in the user's PC in a hidden form. Card readers used by e-COMM are basic smart card readers, even if e-COMM may also use secure smart card readers.

For micro-payments, the ambition of e-COMM could be to make a 'micro-SET' standard. The e-COMM solution is a post-paid payment system and uses the same 'CB' bank card as for normal payments. Indeed, the use of the SET protocol for e-COMM micro-payment is not possible mainly because of the cost of clearing and settlement of micro-transactions if processed one by one. The micro-payment system is based on an aggregation of micro-transactions for charging the buyers and paying the merchants. There is also a flow control mechanism by an authorisation ceiling delivered through a normal authorisation: SET transaction without capture. Aggregation and flow control are performed by an entity called 'intermediary', which may be operated by banks, by telecom operators, or both. Critical messages are secured using the SET certificates and keys of the buyers, merchants and intermediary.

The e-COMM consortium includes Visa International, BNP, Société Générale, Crédit Lyonnais, France Télécom and Gemplus. The consortium is currently setting up a pilot where Gemplus acts as a certification operator for the e-COMM banks, cardholders and merchants. Groupement Carte Bleue[3] should have the role of a certification authority for it's member-banks and for the French e-COMM payment

[3] 'Carte Bleue' is a card brand with access to the Visa network (number two of Visa's worldwide card sales volume). Groupement Carte Bleue manages the clearing system between Carte Bleue Member banks for French domestic transactions. It manages the gateway for authorisations between France and Visa. It manages the clearing system between Carte Bleue banks and Visa for interchange transactions.

servers. Gemplus will deliver Visa-brand digital certificates on behalf of Groupement Carte Bleue, in conformity with the SET standard.

5.1.3 Issues

1. Both projects plan a second phase with EMV standard cards. For processing SET certificates, the chip card will have to support the RSA cryptosystem using a 1024 bit modulus and provide high memory capacity. It is not sure that the next coming smart card generation will be able to contain the full SET certificate, providing real mobility. In addition to these technical problems, there are potential cost problems.
2. The question of the standardisation of the smart card readers is important too. Actually C-SET requires a specific card reader whereas e-COMM needs only a basic one. E-COMM (maybe more than C-SET) seems to rely on:
   - a rapid popularisation of the smart card readers e.g., into PC's. (see PC/SC workgroup [PC/SC]),
   - the smart card trend of SET
   - the increase of the smart card capacities.

   In the current stage, one can guess C-SET and e-COMM will agree on compatible devices for their pilots.
3. The future 2.0 release of the SET specifications might facilitate (incite?) the use of smart cards with the SET protocol. If C-SET decides to comply with these specifications there will be a good chance to see a convergence of C-SET and e-COMM. The EMV standard should also encourage this convergence.

5.2 MANDATE II

MANDATE II [Mandate] is a project under the EC DGXIII ETS (Electronic Trusted Services) programme currently developing an electronic cheque. It is the intention of the project to create an electronic negotiable instrument mirroring all the functionality of a paper cheque.

Central to the technical solution is a 'DOC-carrier' (DC), which is tamper-resistant and implemented in some special hardware such as an advanced smart card. The DC can be thought of as an electronic chequebook and is initialised by the issuing bank by entering account information etc. Furthermore two public key pairs are generated (one for signing and one for encryption) and certificates on the keys are issued.

5.2.1 Background

The goal to achieve is that an electronic cheque - or rather, an electronic realisation of a cheque - at any particular time can be proved to be the (temporary) property of a particular user. With ordinary paper documents, giving the original of a document certain physical attributes that are difficult to reproduce solves the problem. With this precaution, it makes sense to speak of the original of a document, and define the owner simply as the person holding the original.

The important properties required are *uniqueness* and *ownership*. The problem is to find a suitable attribute on an electronic cheque, which somehow would give it the property of uniqueness, explicitly or implicitly in such a way that it makes sense to talk about being the rightful owner of the cheque.

Obviously, the concept of a paper-based original does not make sense for electronic documents, and other (e.g. cryptographic) methods must ensure that the owner of a particular electronic cheque can be identified.

Any document of some value must initially be generated by someone, who will guarantee its value. This requires the proof of, or non-repudiation of, origin service (one example is electronic cash), which is a well known art and realised using digital signatures.

An electronic cheque contains information on amount etc. and a digital signature by the issuer on this information making the cheque valid. In fact the (verifiable) signature is the piece of information that has the value. The question now is how to develop a protocol to cover the situation, where a cheque, once issued, is to change hands. The main problem is to ensure, that the new owner is uniquely identified, or, in other words, that the payee cannot circumvent the measures and sell the same cheque (the issuer's valuable signature) to two different entities.

5.2.2 The Use of Tamper Resistance to Achieve Uniqueness

To realise freely negotiable electronic documents has only been analysed very recently in the literature, in the TEDIS II B7 report, "Security in Open Environments" (1993), and the subsequent TEDIS II report, MANDATE, on electronic negotiable documents, where the general principles, but no specific solution, are given. In the following, we give a brief overview of the requirements defined in these reports.

The only practical way to provide uniqueness is to physically prohibit free copying. This would involve tamper resistance to realise a protected communication with restricted functionality, if possible.

The basic principle for achieving ownership and uniqueness here is simple but fundamental:

Ownership: A message encrypted under a key known to only one entity belongs to that entity, as long as it is encrypted, and establishes indisputable ownership by the mere fact that it will only be useful to the owner of the key. Only the person in possession of the right key can make any use of the document, which in effect is the property of ownership. The rightful owner of a cheque is the person being able to present the issuer's (decrypted) verifiable signature.

Uniqueness: On the other hand, the only way the rightful owner can verify the encrypted signature of a cheque is by decrypting it. But this will give him access to the signature and he may subsequently be able to sell the cheque to two different persons by encrypting the signature with their respective keys. To achieve uniqueness this must be prevented by protecting the valuable signature using tamper-resistant hardware, perhaps a chipcard, or a hardware protected PC.

In MANDATE this tamper-resistant hardware is called the DOC-carrier. Its properties will be described in detail.

5.2.3 The MANDATE Cheque System

The MANDATE cheque system has the following properties:

Cheques are generated electronically on the tamper-resistant DC. This requires some care. It is essential that the signatures generated to provide the non-repudiation is never disclosed. It is of course sufficient to represent each cheque by a hash value and the generating digital signature inside the DC. The message itself does not need to be protected.

A cheque is transferred from one DC to another, through a public unprotected network (e.g. by e-mail), in such a way that the following properties hold:

- It can only be transferred as a meaningful document to one particular DC chosen from any number of DCs
- The protocol cannot be completed by any other device than an authorised DC.
- The system is completely open to communication between any two DCs, without bilateral agreements.

Each DC "possesses" two public key pairs; one for signing and one for encryption. The secret keys are not known even to the owner of the DC. The secret key is generated on the DC and never leaves it unprotected, hence not even the system provider knows the secret keys of the DC.

The cheque consists of the information (payee, amount, timestamp, expiration date etc.), and the corresponding digital signature, calculated by means of the secret key of the payer and a hash value of the information.

Now, the problem is that this shall only be released through a selling process to another DC. So the question is, how can one DC identify another?

In MANDATE the public key of the CA is installed on each DC, along with the before-mentioned key-pairs. When a document, or rather the corresponding key protected signature, is entered on the DC, the DC software ensures that it can only be released again encrypted under a public key certified by the CA (and verified by means of the corresponding public key on the DC). The point behind this is that it will prevent the use of a non-authorised DC to get access to the vital signature that defines the cheque. In particular this encrypted message is useless except when imported into the DC holding the corresponding secret key. It is thus important to realise that the value of the cheque is represented by the digital signature of the issuer.

Furthermore, and this is an essential property, such an encryption of a particular cheque on an individual DC can take place only once, or rather, once a public key has been selected, it is impossible at any later stage to go through the same procedure with another public key.

Whenever issuing a cheque, a copy is sent to a Trusted Third Party (TTP) that holds copies of the secret encryption keys. In case of loss or faults the cheque can be recovered by the TTP. This can not be done until after the expiration date to prevent fraud.

5.2.4 The Pilot Project

A pilot project is currently being carried out with participation of three European Banks, viz. Nordvestbank, Denmark, Royal Bank of Scotland, and ING Bank, The Netherlands. In the pilot a software-only implementation is used to test the functionality of the electronic cheque concept.

6 Conclusions and Outlook

State of the art technology enables secure electronic payment systems running over the Internet. Cryptography can provide procedures for confidentiality, authentication, non-repudiation and anonymity. PKIs maintain the public keys of all the players and thus support authentication and non-repudiation in an open environment. Secure user devices can store data like private keys in a tamper-resistant device, e.g., a smart card. Electronic wallets with secure access to a display and keypad provide additional security by preventing Trojan Horse attacks.

Direct account-based payment systems are used most frequently on the Internet. These payment systems comprise credit-card and e-cheque transactions. New protocols for these payment systems tend to take full advantage of the security technology and rely on multi-party protocols, public key infrastructures and secure user devices.

Several protocols exist for credit-card payments. SET is currently not in commercial use, but we expect SET to become a dominant protocol within the next years. SET specifies a multi-party protocol and a global public key infrastructure. There is a clear trend to secure user devices, e.g., smart cards, as already supported by the SET variants C-SET and e-COMM. General support for smart cards is expected to be specified in the next version of SET.

A similar trend can be noticed for e-cheque payment systems. New e-cheque payment systems will rely on public key infrastructures and secure user devices. The most promising e-cheque systems are MANDATE II and the FSTC model. For Europe, MANDATE II is preferable because the FSTC system might be subject to export restrictions. Moreover, MANDATE II supports loss tolerance.

As a next step, the integration of MANDATE II into SEMPER will be considered according to the specifications outlined in this deliverable. In particular, a MANDATE II subclass of *Cheque* will be provided and an adapter will be written to interface with MANDATE II. This will be achieved in close cooperation with the MANDATE II project.

7 References

[AASW98] J.L. Abad-Peiro, N. Asokan, M. Steiner, M. Waidner: **Designing a generic payment service,** SEMPER Public Project Reports; <http://www.semper.org/info/ >, to appear in IBM Syst. Journal, 37(1), January 1998.

[AJSW97] N. Asokan, Phil Janson, Michael Steiner, and Michael Waidner: **State of the art in electronic payment systems**, IEEE Computer, 30(9): pp. 28-35, September 1997.

[CAFE] **Secure International Payment and Information Transfer**, *Principle Results from the Initial Survey Scenarios, Frankfurt 1995.*

[Ch82] D. Chaum: **Blind Signatures for Untraceable Payments;** Advances in Cryptography, Crypto '82 (Eds.: D. Chaum, R.L. Rivest, A.T. Sherman), Plenum Press, NY 1983, 199-203.

[D03] **Basic Services, Architecture and Design,** *SEMPER Public Deliverable D03; Aug 31, 1996; <http://www.semper.org/info/>.*

[D14] **Architecture of Payment Gateway,** *SEMPER Public Deliverable D14; November 22, 1996; <http://www.semper.org/info/>.*

[GA31] **Genfer Abkommen über das einheitliche Checkgesetz**, vom 19. März 1931, SR 0.221.555.1.

[L82] L. Longpré: **The Use of Public-Key Cryptography for Signing Checks**; Advances in Cryptography, Crypto '82 (Eds.: D. Chaum, R.L. Rivest, A.T. Sherman), Plenum Press, NY 1983, 187-197.

[NM95] B.C. Neuman, G. Medvinsky: **Requirements for network payment: the NetCheque Perspective**, *IEEE COMPCON '95, March 5 - 9, 1995, San Francisco, CA, USA, pp. 32-36.*

[rfc1898] **Request for Comments: 1898**; CyberCash Credit Card Protocol Version 0.8

[S97] M. Sirbu: **Credits and debits on the internet**, *IEEE Spectrum, Special Issue: Electronic Money, Feb 1997 (cf. <http://www.spectrum.ieee.org>).*

[ST95] M. Sirbu, J.D. Tygar: **NetBill: an internet commerce system optimized for network delivered services**, *IEEE COMPCON '95, March 5 - 9, 1995, San Francisco, CA, USA, pp. 20-25.*

http references (subject to changes):

[COM97] *http://www.ispo.cec.be/Ecommerce/ (A European Initiative in EC)*

[C-SET] *http://www.eurocardmastercard.tm.fr/us/commerce/f-commerce.htm* (Cybercard)

[e-COMM] *http://www.e-comm.fr* (e-COMM)

[ECheque] *http://sedam.mkn.co.uk/help/bank/echeque* (ECheque)

[ECOMM] *http://www.iitf.nist.gov/eleccomm/ecomm.htm (A Framework for Global Electronic Commerce)*

[EMV] *http://www.mastercard.com/emv* (Europay, Mastercard, Visa: specifications for cards, terminals and applications)

[FSTC] <*http://www.fstc.org/projects/echeck/*> (Electronic Check Proposal)

[Mandate] <*http://www.cryptomathic.dk/mandate*> (MANDATE)

[NetBill] *http://www.ini.cmu.edu/netbill/* (NetBill)

[NetBilla] <*http://www.netbill.com/netbill/security-crypto.html*> (NetBill Security)

[NetCheque] *http://nii-server.isi.edu/info/NetCheque/* (NetCheque)

[PayNow] *http://www.cybercash.com/cybercash/paynow/* (PayNow)

[PC/SC] *http://www.smartcardsys.com* (PC/SC workgroup : Specifications for PC-ICC Interoperability)

[Redi-Check] *http://www.redi-check.com/info/consumer_info.html* (Redi-Check)

[SET97] Mastercard, Visa: Secure Electronic Transactions: <*http://www.mastercard.com/set/set.htm*> and <*http://www.visa.com/cgi-bin/vee/nt/ecomm/*>.

[SSL] *http://www.netscape.com/info/security-doc.html* (Netscape Security)

8 Appendix

8.1 Specification of Cheque-Related Classes in the Payment Block

The documentation of the sub-interface for the use of electronic cheques in *SEMPER* is public and available on-line. The documentation has been generated from the source code using JAVADOC which produces a document in the HTML format. To access the documentation, one needs to input the so called URL as “Location” to the browser. HTML copies with the description of the new classes in the SEMPER payment block can be found at URL:

<http://www.semper.org/deliver/d15/javadoc/index.html>.

8.2 Glossary

Acquiring bank
The bank or financial institution of the payee in an electronic payment system.

Anonymity
A player (Alice) is said to be anonymous against another player (Bob) if Alice's real identity is not revealed to Bob, e.g., by using a pseudonym.

Authentication
A proof of identity. This proof can be related to a message being sent meaning that a proof of origin is sent along (see also digital signatures).

Certificate
A certificate is a digitally signed statement about a person. *SEMPER* distinguishes three types of certificates: key certificates linking a public key to a person, attribute certificates linking a particular property to a person and hybrid certificates linking both a key and an attribute to a person.

Confidentiality
Protecting a message against eavesdropping such that it is only meaningful to the intended entity or set of entities.

Clearing
The sorting of payments between banks or financial institutions, initiation of the delivery process and capture of the settlement information.

Deposit a cheque
A cheque is deposited by transferring it to the acquiring bank to claim a credit for the stated amount.

Digital signature
A digital signature is an electronic counterpart of a hand-written signatures. It is verified against a public key, and if the signature system is secure, this serves as a proof that the signed message originates from someone knowing the corresponding secret key.

Draw a cheque
Completion of a cheque for payment: the payer specifies the amount and signs the cheque before it is passed on to the payee.

Electronic money
Electronic money is the electronic counterpart to the conventional money.

Endorse a cheque
Instead of depositing a cheque, the right to the funds is passed on to another person or business. The endorsed cheque is used as a payment.

Identification
A process whereby an entity proves its identity.

Integrity protection
The protection of information against changes by intruders (tampering).

Issuing bank
The bank or financial institution of the payer in an electronic payment system.

Non-repudiation
Non-repudiation means that a party cannot falsely deny later that a certain event or action took place. One mechanism to achieve non-repudiation is the use of digital signatures.

On-line payment system
On-line payment systems involving a third party for payments from the payer to the payee (authentication and authorisation server, usually at the issuer or acquirer side).

Payee
The role played by someone receiving money in a payment.

Payer
The role played by someone paying in a payment.

Pay-later payment system
In pay-later payment systems the payer's account is debited after the payment (i.e., in contrast to a pre-paid payment system). Credit-card payments fall in this category.

Payment system
A set of instruments and banking procedures that support the transfer of money.

Payment system provider
A party (such as a financial institution) that makes a payment system available.

Player
A player is a real-world person or body participating in the electronic marketplace, e.g. a payer, a payee or a third party like a payment system provider, a notary service, etc.

Pre-paid payment system
In pre-paid payment systems the payer's bank account is debited an amount that afterwards can be used for payments.

Revocation of a certificate
The process of withdrawing the validity of a certificate. A certificate is revoked by the certification authority. The reason could be that the key is compromised, lost, or was registered by an impostor or that the user abused the granted rights.

Security
Security is used in two different meanings:
a) Security of a payment system means an assurance of the correctness of the payment system provided by technical measures and banking procedures.
b) A security is a financial instrument, which gives its owner a particular right; e.g., a drawn cheque provides the right to get the stated amount at an acquiring bank.

Settlement
The actual exchange of funds between the banks or financial institutions, usually through account entries at the central bank.

Unlinkability
In addition to anonymity, unlinkability means that Bob cannot link two or more actions of Alice.