Electronic Payment over Open Networks — A Technology Overview —[1]

P. Janson, M. Waidner
IBM Zurich Research Laboratory
CH 8803 Rüschlikon, Switzerland
{pj,wmi}@zurich.ibm.com

Version 5/8/95

Abstract: As business is moving from face-to-face trading, mail order and phone order to electronic commerce over open networks such as the Internet, crucial security issues are being raised. While Electronic Funds Transfer over financial networks is reasonably secure, securing payments over open networks connecting commercial servers and consumer workstations poses challenges of a new dimension. This paper reviews the state of the art in payment models and technologies, and sketches emerging developments.

1 Introduction

Since the dawn of history there was trading between two parties exchanging goods face-to-face. Eventually such trading became complicated and money was invented so a buyer could acquire something he needed from a merchant without necessarily exchanging goods. Security of the monetary systems was guaranteed by the local, regional, national and eventually international banks controlling the printing of money. New steps were taken when payment orders, cheques, and later 'plastic' money were invented. This allowed payment without 'actual' money, the mapping between the payment instrument and the real money being still guaranteed by the banks through secure financial clearing networks. Eventually remote payment became possible using those same instruments, although security then started to become a challenge. Indeed verifying a signature on a cheque or a credit card mail order when buyer and merchant are not face-to-face is impossible: either the buyer must take the risk of sending in a payment before having received his purchase or the merchant must send the purchased items before having received the payment. Phone order purchases are even worse since no signature at all can be provided: the merchant runs the risk that the buyer may deny having made the purchase and demand a refund even after he has received the goods. Without new security measures, envisioning electronic commerce over open computer networks is utopic. This paper discusses electronic payment models in Section 2, security requirements in Section 3, and emerging technologies in Section 4.

[1] In the following, most references are URLs, pointing to the *World Wide Web*. All these on-line references can be accessed via <http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/>.

2 Electronic Payment Models

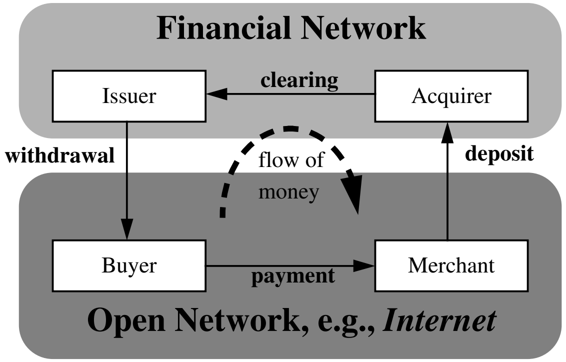

Figure 1 Basic components of a payment system. In principle, all transactions could be performed via the open network, but for security and historical reasons, the existing financial networks will be used for clearing.

Commerce involves always a **buyer** and a **merchant** who need to exchange money for goods or services, and at least one financial institution which links "bits" to "money." In most existing payment systems, this role is divided into two parts, an **issuer** (used by the buyer) and an **acquirer** (used by the merchant).

The electronic payment from buyer to merchant is implemented by a flow of real money from

- buyer to issuer (*withdrawal*, e.g., by buying a phone card using cash, or by moving money out of a debit account, or into a credit account),
- issuer to acquirer (*clearing*),
- acquirer to merchant (*deposit,* e.g.,by putting money into the merchant's account).

In *pre-paid (debit) payment systems,* the bank account or real purse (if loading cash via a reverse ATM is possible) of the buyer is debited a certain amount which can be used for payments afterwards. Card-based electronic purses, electronic cash as well as (certified/guaranteed) bank cheques fall in this category. In *pay-now payment systems*, the buyer's account is debited at the time of payment. ATM-card based systems (like the European edc-system) fall in this category. In *pay-later (credit) payment systems*, the merchant's bank account is credited the amount of the sale before the buyer's account is debited. Credit card systems fall in this category.

3 Security Requirements

The security requirements of electronic payment systems vary depending on their features and the trust assumptions put on their operation. Therefore, it is not possible to provide a single specification how to secure them. Generally, though, one or more of the following illustrative requirements must be met:

Integrity and authentication:

- Messages that authorize debit of a buyer's account need to be *signed* by that buyer to guarantee that unauthorized parties, including the issuer itself, cannot draw on the buyer's account without an explicit proof that the buyer authorized the debit.
- Both the buyer and the banks involved want to make sure that such signed payment authorizations are unique and cannot be submitted twice by a claimed merchant.
- The buyer may demand from the merchant a signed acknowledgement that the purchased goods or services were or will be delivered (on-line or off-line depending on the kind of merchandise purchased).
- Buyer and merchant may in fact want a trusted third party to insure fair exchange of the payment for the above signed acknowledgement.
- The merchant may want from the acquirer a guarantee of payment before any goods or services are actually provided to the buyer.

Confidentiality:

- Some or all parties involved may wish confidentiality of the transaction, whereby identity of the buyer, merchant, purchase content, amount, etc., are known only to the participants involved, or even only to a subset of them (e.g., where untraceability is desired).

Availability and Reliability:

- All parties are interested in being able to perform payments whenever necessary.
- Payment transactions must be atomic, i.e., happen entirely or not at all, but never hang in an unknown or inconsistent state. No buyer would accept to lose money due to a network crash, or because the merchant's server crashed.

  Availability and reliability presuppose that the underying networking services and all software and hardware components are sufficiently dependable. Recovery from crash failures requires some sort of stable storage at all parties and specific resynchronisation protocols. These fault tolerance issues are not discussed in the following, since most payment systems do not address them explicitly.

To address the security requirements, digital signatures and secret key distribution functions are required, which makes it desirable that all parties involved have access to secure key storage. If payments are to be possible from any workstation, the secret key storage of a user must even be mobile, which in turn makes it necessary that users be provided with smart cards or similar secure devices. These technology options are discussed in the following Section 4, together with some examples.

4 Technology Overview

The main design decision for electronic payment systems is how to authorise payments, i.e., how to enable the honest buyer to convince the merchant to accept a legitimate payment while preventing the dishonest buyer from doing unauthorised payments. For instance, it must not be possible to spend the same money twice by sending the same messages to two different merchants. And all this must be done in a way that does not harm the privacy of honest buyers and merchants.

This short of technology overview is structured according to the different techniques used to solve this problem. Thereby, we split the problem into two sub-problems:

- The buyer is *authenticated* as a "legal" payer (e.g., by means of a public-key certificate), and the merchant or acquirer are convinced by some protocol that *if* the buyer is honest, *then* the merchant will receive the money.
- The payment is *authorised,* i.e., the merchant is convinced that he will receive the money.

4.1 On-line vs. off-line

Payments can be performed *on-line*, involving an authentication and authorisation server (usually as part of the acquirer) in each payment, or *off-line*, i.e., without contacting a third party during the payment from buyer to merchant.

On-line systems require, of course, more communication, but not necessarily specific tamper-resistant hardware at the buyer and merchant. In general, they are considered as more secure than off-line systems. Most proposed *Internet* payment systems are on-line systems.

Off-line *authorisation* systems are more communication efficient, but usually require tamper resistant hardware at the buyer (e.g., smartcards) and sometimes also at the merchant (e.g., security modules of POS-terminals).

All proposed *electronic purses* follow this concept, e.g., *Danmont, Proton* (by *Banksys*), *Mondex*[2], *Express* (by *Europay*), *CAFE*[3] (developed by a European ESPRIT consortium). The "exotic" systems in this list are *Mondex* and *CAFE*. *Mondex* is the only system that enables off-line transferability (i.e., the merchant can use the amount received for a new payment, without intermediate deposit — but this seems to be a politically unpopular feature in most countries), and it is the only system considered for high-value payments (i.e., beyond 100 ECU). *CAFE* is the only system that provides strong buyer anonymity and untraceability. Both systems offer the buyers an *electronic wallet*, preventing the well-known fake-terminal attacks on the buyer's PIN. *Mondex, Express*, and *CAFE* are multi-currency purses, i.e., they can handle different currencies simultaneously.

All these systems could be used for Internet payments, but currently, they aren't. The main

[2] <http://www.mondex.com/mondex/home.htm>; see also *Richard Rolfe:* **Here Comes Electronic Cash;** Credit Card Management Europe, January/February 1994, 16-20.

[3] <http://www.zurich.ibm.ch/Technology/Security/sirene/projects/cafe/index.html>; see also *Jean-Paul Boly* et.al.: **The ESPRIT Project CAFE - High Security Digital Payment Systems;** ESORICS '94, LNCS 875, Springer-Verlag, Berlin 1994, 217-230.

obstacle is that they require a smartcard reader attached to the buyer's PC or workstation. Inexpensive PCMCIA smartcard readers and standardised infrared-interfaces on notebook computers can solve this connectivity problem. This is the approach taken in the recently announced *First Bank of Internet*[4] system, based on the newly announced VISA electronic purse.

Another system that will be developed in this spirit is the *FSTC Electronic Check*, that will use a tamper-resistant PCMCIA card, and will implement a cheque-like payment model.

Alternatively to tamper-resistant hardware, off-line authorisation could be done via *pre-authorisation*, i.e., the merchant is known in advance, and the payment is already authorised during withdrawal, in a way similar to a certified bank cheque.

Whether off-line *authentication* requires tamper-resistant hardware or not, depends on the cryptographic primitives used, and on how trustworthy the buyer's PC or workstation is from the buyer's point of view.

4.2 Tamper-resistant Hardware

As already mentioned in Section 4.1, for the issuer's security, most off-line payment systems require a piece of tamper-resistant hardware in the buyer's device. In a certain sense, this piece is a "pocket branch" of the issuer.

Independent of the issuer's security considerations, it might also be in the buyer's interest to have a secure device, protecting the buyer's secret keys. Initially, this could be just a smartcard, but in the long run, it should be at least a smartcard reader with its own keyboard and display for entering a PIN and simple commands. This is often called an *electronic wallet*.

Without such a secure device, the buyer's secrets, i.e., the buyer's money, are vulnerable to anybody who can access the buyer's machine. This is obviously a problem in multi-user environments, but also on single-user machines that may be accessed directly or indirectly by others, and where a virus, for instance, could steal PINs and passwords while they are entered.

Even with a smartcard, the buyer cannot be sure that a Trojan horse in his or her PC cannot reveal PINs of credit cards by sending mail to a remote attacker, or by simply asking the smartcard to make a payment to the attacker's account, silently. Therefore, for real security trusted input and output channels between user and "pocket workstation" must exist, e.g., using an electronic wallet with its own display and keypad.

4.3 Cryptography

"Crypto-less" Systems

Using *no cryptography* at all means relying on "out-band" security: For instance, the goods ordered electronically are not delivered before a fax (or a letter, or a phone call) arrives from the buyer that acknowledges this order.

Examples for this kind of systems are *CompuServe, First Virtual*[5], and the *Internet Shopping*

[4] Announcement <http://catless.ncl.ac.uk/Risks/16.93.html#subj11>

	Cryptography used	System	Comments	
Off-line systems	Shared-key cryptography	*Danmont*, *Proton* by *Banksys*		Pre-paid "electronic purse" systems. Security depends on cryptography *and* tamper-resistance of smartcards or electronic wallets.
	Not known	*Mondex*		
	Public key cryptography	*Express* by *Europay*		
		CAFE (ESPRIT Project)	Untraceable payment system.	
On-line payment systems	Crypto-less systems	*First Virtual*	Used for small values and information services only.	Post-paid, credit card based.
		Internet Shopping Network		
	Generic Concept	*Payment Switch* by *OpenMarket*	Suitable to implement different payment models. Actually, OpenMarket uses at the customer shared-key cryptography only.	
	Shared-key cryptography (*Kerberos/DES*)	*NetBill* by *CMU*	Both systems aim at small ("micro") payments. No non-repudiation.	
		NetCheque by *USC*		
	Public-key cryptography (*RSA*)	*ecash* by *DigiCash*	Untraceable payment system.	Pre-paid "electronic cash".
		CyberCash		Post-paid, credit card based.
		iKP by *IBM*	Actually a family of protocols. 3KP provides full non-repudiation.	

Figure 2 Overview of payment systems mentioned in the following. Systems that are not implemented are omitted.

Network[6]. In *CompuServe*, each customer uses a line to dial into the system that is assumed to be secure by itself, and identifies himself or herself to the system. For both *First Virtual* and the *Internet Shopping Network*, the buyer has an account with the system and receives a password in exchange for a credit card number. The password is not protected while travelling over the *Internet*, i.e., these systems are vulnerable against eavesdropping. *First Virtual* has some protection by asking the supposed buyer for an acknowledgment of each payment via email, but the actual security of the system is based on the fact that buyers can revoke *each* payment within a certain time (i.e., there is no definite authorisation during the payment).

[5] <http://www.fv.com>

[6] <http://www.internet.net/>

Generic “Payment Switch”

A special role is played by the *OpenMarket Payment Switch*[7]: It is an on-line payment system implementing both, a pre-paid and pay-later models. It supports *several* authentication methods, depending on the payment method chosen, ranging from simple, unprotected PIN-based authentication to challenge-response based systems, where the response is computed, e.g., by a smartcard.

Actually, *OpenMarket* uses passwords and optionally two types of devices for response generation, *Secure Net Key* and *SecureID,* i.e., shared-key cryptography. (For authorisation, the *Payment Switch* digitally signs an authorisation message sent to the merchant, i.e., public-key cryptography is used for this special purpose.)

Shared-key Cryptography

For *shared-key cryptography***,** the buyer and merchant on the one side and that party performing authentication or authorisation on the other side need a shared secret (e.g., a DES-key[8], or at least a password/PIN).

Since both sides have exactly the same information, this cannot provide *non-repudiation* (e.g., if buyer and issuer disagree about a certain payment, there is no way to decide whether this payment was initiated by the buyer, or by a dishonest employee of the issuer), and is therefore not recommended for high-value payments (say, greater than 100 ECU).[9]

If authentication should be done off-line (which is desirable at least for low-value payments), each pair of buyer and merchant need a shared secret key. In practice this means that some sort of master-key is present at each merchant, enabling the merchant to derive the buyer’s key, e.g., from the buyer’s identity. Usually, tamper-resistant security modules in point-of-sale terminals are used to protect this key.[10]

Shared-key cryptography is used, e.g., by the off-line systems *Danmont* and *Proton,* and the on-line systems *SNPP*[11], *NetBill*[12] (by *Carnegie Mellon University, CMU*), and *NetCheque*[13] (by *University of Southern California*).

NetBill and *NetCheque* are based on the Kerberos technology, and focus on “micro-payments.” Both implement a cheque-like debit payment model. The use of shared-key technology is justified by the performance required to process many micro-payments in short time.

In February 1995, *VISA* and *CMU* announced a cooperation to develop *NetBill*, probably in the direction of using asymmetric cryptography, for commercial purposes.

Public-key Cryptography

For *public-key cryptography,* the buyer has a secret signature key and a certificate for his corresponding public signature verification key (e.g., issued by the payment system operator or a specific issuer). In most existing and proposed systems, *RSA* is used (but there are several alternatives).

Digital signatures provide *non-repudiation*, i.e., disputes between sender and recipient of a signed message can be resolved. This should be mandatory at least for high-value payments.

Off-line *authentication* is no problem here, since the merchant can easily verify a signature of the buyer (and could check the certificate against a local copy of a blacklist of “bad” certificates, if necessary). Authorisation still requires either an on-line connection or trusted hardware at the buyer.

Public-key cryptography will be used, e.g., by the off-line systems *Express* (by *Europay*) and *CAFE*. Most of the proposed on-line payment systems use public key cryptography:

Rather *general WWW security schemes* using public-key cryptography are *SHTTP*[14] and *SSL*[15]. Neither is a payment technology per se, but they are suggested for securing also payment information.

SSL is an Internet socket-layer communication interface allowing buyer and merchant to communicate securely. *Netscape Communications Corporation* (which proposed *SSL*) is offering payment mechanisms based on that secure interface. *SSL* does not support non-repudiation.

SHTTP is a secure extension of the HTTP protocol used on the Internet *World-Wide Web* (WWW)[16], developed by the *CommerceNet*[17] consortium. *SHTTP* offers several security techniques, e.g., signing and encrypting with RSA, on top of which various payment protocols may and will be implemented.

Both SSL and SHTTP offer a selection of symmetric and asymmetric cryptographic technologies. Because of the open access these technologies offer to strong cryptographic primitives, they are all subject to U.S. export restrictions. Exportable versions will be available but they will be using ‘tamed’ (less secure) cryptographic technologies. It is very questionable whether banks, merchants, and customers outside North America will be interested in such ‘second-grade’ technologies.

Complete payment systems using public-key cryptography are, e.g., *ecash*[18,19] (by *DigiCash*), *NetCash*[20,17] (by *University of Southern California*), *Cybercash*[21], and *iKP*[22] (by *IBM*).

---

7 <http://www.openmarket.com/about/technical/>*:* see also: *David K. Gifford, Lawrence C. Stewart, Andrew C. Payne, G. Winfield Treese:* **Payment Switches for Open Networks;** IEEE COMPCON, March 95.

8 We do not provide references to cryptographic algorithms in this overview. For an introduction and a description of most of the cryptographic algorithms used for electronic payment systems, see *Bruce Schneier:* **Applied Cryptography;** John Wiley & Sons, 1994.

9 For some examples on the consequences of *no* non-repudiation see: *Ross Anderson:* **Why Cryptosystems Fails;** Communications of the ACM 37 11, November 1994, 32-41. <ftp://ftp.cl.cam.ac.uk:/users/rja14/wcf.ps.Z>

10 For an example, see: **Integrated Circuit Card Specifications for Payment Systems;** Europay/MasterCard/VISA, October 1994.

11 *Semyon Dukach:* **SNPP: A Simple Network Payment Protocol;** Computer Security Applications Conference,1992. <ftp://ana.lcs.mit.edu/pub/snpp/snpp-paper.ps>

12 <http://www.ini.cmu.edu/netbill>; see also: *Marvin Sirbu, J. D. Tygar:* **NetBill: An Internet Commerce System;** IEEE COMPCON, March 95 <http://www.ini.cmu.edu/netbill/CompCon.html>.

13 *Clifford Neuman, Gennady Medvinsky:* **Requirements for Network Payment: The NetCheque™ Perspective;** IEEE COMPCON, March 95. <ftp://prospero.isi.edu/pub/papers/security/netcheque-requirements-compcon95.ps.Z>

14 *Secure HyperText Transfer Protocol;* see <http://www.eit.com/projects/s-http/>

15 *Secure Socket Library;* see <http://www.mcom.com/info/SSL.html>

16 <http://www.w3.org/>

17 <http://www.commerce.net/>

18 <http://www.digicash.nl/>

19 See Section 4.2.

20 <http://nii.isi.edu/gost-group/products/netcash/>

In November 1994 *VISA* and *Microsoft* announced a common plan to develop and offer secure payment technology based on *RSA* technology, but not much more is publicly known about the design as of this writing.

IBM is developing an open payment technology, *iKP*, implementing a credit-card-like payment model that easily connects to the existing credit card clearing networks. The payment logic is bundled with strong cryptographic mechanisms that are not accessible to other applications. The objective is that such a design should be exportable according to the U.S. law and importable to almost any other country, thus forming a valuable basis for an internationally usable open and secure technology. Furthermore, the technology is designed so that it can operate transparently with any WWW browser and server on any platform, unlike some other designs that require specially equipped browsers and servers.

4.4 Anonymity of Buyer

Some payment systems provide buyer anonymity and untraceability. Both are considered useful for cash-like payments (say, up to 100 ECU), with the argument that real cash is also anonymous and untraceable, and that buyers do not want to enable a third party to trace all their everyday-payments, certainly not the merchants (shops, publishers, etc.), but in some cases not even the banks.

While *anonymity* simply means that the buyer's identity is not used in payments, *untraceability* means that the buyer cannot be identified, and even that two different payments of the same buyer cannot be linked. Both properties hold with respect to the merchant only or with respect to both merchant and issuer/acquirer.

All payment systems could made untraceable by *outsiders,* by encrypting all flows between buyer and merchant, and anonymous to merchant by using pseudonyms instead of real identities.

Some electronic payment systems are designed in a way which provides anonymity or even untraceability with respect to the merchant (e.g., *iKP*[20] offers this as one option).

Currently the only payment systems mentioned here that provide anonymity and untraceability against merchant *and* issuer/acquirer are *ecash*[16] (on-line) and *CAFE*[3] (off-line, based on smartcards), both based on asymmetric cryptography (a special form of signatures called *blind signatures*[23]).

NetCash[17] and *ACC*[24] also provide anonymity and untraceability, but based on the use of trusted "mixes" that change electronic money of one representation into another representation, without revealing the relation. Neither *ecash* nor *CAFE* assume the existence of such trusted third parties.

---

21 <http://cybercash.com/>

22 <http://www.zurich.ibm.ch/Technology/Security/extern/ecommerce/>; see also: *Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Michael Waidner:* **iKP — A Family of Secure Electronic Payment Protocols;** IBM T.J. Watson Research Centre and IBM Zürich Research Lab, *Draft*, March 1995.

23 *David Chaum:* **Achieving Electronic Privacy;** Scientific American, August 1992, 96-101. *David Chaum:* **Privacy Protected Payments;** SMARTCARD 2000, North-Holland, Amsterdam 1989, 69-93.

24 <http://www.research.att.com/index.html#acc>; see also: *Steven H. Low, Nicholas F. Maxemchuk, Sanjoy Paul:* **Anonymous Credit Cards;** 2nd ACM Conference on Computer and Communication Security, Fairfax 1994.

5 Summary and Outlook

Because of the limited space in this article, we were not able to describe the technical details of the different payment systems listed. However, even the high-level overview and the rich set of references should have made it clear that the *technology* that is necessary for secure electronic *Internet* payment systems already exists. Achieving security for all parties, inclusive perfect untraceability for the buyer, is possible.

Currently, no proposal or system is dominant, but with high probability this will change within the next two years at most. But the question "Which payment system will be used on the *Internet*?" will not have a single answer. Several payment systems will coexist:

- Micro-payments (less than 1 ECU), low-value payments (1-100 ECU) and high-value payments have significantly different security and cost requirements.

  Possibly, high values will be transferred using non-anonymous, on-line payment systems based on asymmetric cryptography, implementing a cheque-like or credit-card-like payment model. As soon as smartcard readers are available at PCs and workstations, small amounts might be paid using pre-paid off-line payment systems that provide a certain degree of untraceability (like real cash).
- Payment systems with and without tamper-resistant hardware at the buyer will coexist for some time. Ultimately, payment systems based on smartcards and electronic wallets (having their own display and keyboard, and communicating with the buyer's terminal via an infrared interface) will become dominant, since they clearly provide better security and enable the buyer to use untrusted terminals without endangering security.
- Probably, a few almost equivalent payment systems will coexist for the same areas of application (i.e., payment model and maximum amounts). The reasons are various "cultural" differences in the business and payment processes (e.g., between the U.S. and Europe), national security considerations that might disable some solutions in some countries, and competition between payment system providers.

Dr. Philippe Janson teaches at the University of Brussels and is department manager at the IBM Zurich Research Lab. After getting a Ph.D. in operating system security at M.I.T. he worked on the IBM token ring, LAN gateways, heterogeneous network interconnection, and network security, an area in which he has conducted consulting studies for banks in Switzerland. He wrote many papers and a textbook in these fields, and holds several patents and IBM awards.

Dr. Michael Waidner received the Diploma in Informatics and the Dr. rer.-nat. from the University of Karlsruhe in 1986 and 1991, respectively. From 1986 to 1994, he worked for the Universities of Karlsruhe and Hildesheim on different aspects of cryptography, security, reliability, and

fault tolerance. From 1992 to 1994, he worked in the design team of ESPRIT Project CAFE, “Conditional Access for Europe.” Since 1994, he is with the IBM Zurich Research Laboratory in Switzerland. He is (co)author of about 30 papers in cryptography, security, and fault tolerance.