INTERNET-BASED ELECTRONIC PAYMENT SYSTEMS

by

BIRGIT FRIEDERIKE KORTEKAAS

submitted in part fulfilment of the requirements

for the degree of

MASTER OF SCIENCE

in the subject

INFORMATION SYSTEMS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: MRS A J VAN DER MERWE

JOINT SUPERVISOR: MR T J VAN DYK

NOVEMBER 2001

Acknowledgements

To my husband, Kai. Your love and encouragement have given me new significance for every accomplishment. To my mother, sister and brother. You have always been a source of inspiration. And to my supervisor and joint supervisor. Your support and guidance have motivated me throughout the whole year.

INTERNET-BASED ELECTRONIC PAYMENT SYSTEMS

by

B F KORTEKAAS

Degree:	MASTER OF SCIENCE
Subject:	INFORMATION SYSTEMS
Promoter:	MRS A J VAN DER MERWE
Joint Promoter:	MR T J VAN DYK

Summary:

As today, the traditional payment systems of cash, cheques and credit cards are being supplemented by electronic cheques, electronic credit card-based systems, and token-based systems, online security is of utmost importance and one of the biggest criteria used for evaluating electronic payment systems. Electronic payment systems must guarantee the essential security requirements: confidentiality, privacy, integrity, availability, authentication, non-repudiation as well as anonymity and trust. This paper compares the various payment systems (both traditional and electronic) available today mainly according to their security aspects. Secure processing can be accomplished including access controls and detection techniques, such as, encrypted communication channels, user and/or message authentication, symmetric and asymmetric encryption, digital certificates and firewalls. These effective security measures, which are outlined in detail in this paper, will protect the information and payment systems against security risks that currently threaten the Internet.

Key terms:

Internet; electronic commerce; electronic payment systems; authentication; confidentiality; identification; integrity; privacy; security; cryptography; certificates; encryption; digital signatures; anonymity; threats; electronic cash; electronic cheque; smart cards; electronic credit cards

Student number: **3206-125-0**

I declare that **INTERNET-BASED ELECTRONIC PAYMENT SYSTEMS** is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

.....
SIGNATURE
(MRS B F KORTEKAAS)

.....
DATE

Table of Contents

Chapter 4 - Security Aspects

Chapter 5 - Traditional Payment Systems

Chapter 6 – Electronic Payment Systems

Chapter 7 – Traditional Payment Methods versus New Internet "Money"

Chapter 1

Introduction and Overview

1.1 Introduction

Perhaps one of the greatest inventions of our time is the Internet, which has its roots in the Cold War of the early 1960s. Jack Welch, Chairman & CEO of General Electric said:

" I don't think there's ever been anything more important or more widespread...
Where does the Internet rank in priority? It's no. 1, 2, 3, and 4."

Without a doubt, the Internet has had a profound effect on almost every aspect of our lives. The formation of the Internet has changed the way we do business, communicate, entertain and even retrieve information. Nevertheless, the Internet might not have ever materialised if it had not been for "**ARPANET**".

ARPA, which stands for Advanced Research Projects Agency (or more correctly Defense Advanced Research Projects Agency – DARPA) is a military organisation that controls computer research. In the early **1960**'s this agency became very concerned about the possible effects of nuclear attack on its computing facilities and was looking at how they could strategically protect and improve communication systems using computers. They saw a need of being able to share data between their research centres and raised a proposal for packet switching. At the time Dr. Leonard Kleinrock was the leader in such studies, and since he was at UCLA (University of California at Los Angeles), the project was introduced to UCLA.

By **1966/67** the new head of computer research, Leonard Roberts presented his plan for an "ARPANET" at a conference at which he described the reasons for the network and how the network would operate using a sub-net of "interface message processors". The

interface message processors would interconnect, send and receive data, check errors, verify messages and retransmit data in need.

The contract to build this network was awarded to BBN (Bolt, Beranek & Newman Corp.). Around **Labour Day** in **1969**, BBN delivered an Interface Message Processor; the first node of the future APRANET, to UCLA. In **October 1969**, IMPs (Internet Message Processors) were installed in computers at both UCLA and SRI (Stanford Research Institute). APRANET was born!

As more sites were connected the ARPANET expanded rapidly. It was realised that the Network Control Protocol (NCP), the first networking protocol used on the APRANET would need to be replaced by a more independent protocol - TCP/IP (Transmission Control Protocol/Internet Protocol).

In **1983**, the APRANET switched from NCP to TCP/IP, developed by Bob Kahn at DARPA and Vinton Cerf from UCLA. This protocol TCP/IP is still the standard in use on the net today.

In **1990**, "the World" became the first commercial provider for dial-up access. The development of the Internet continued. Tim Berners-Lee developed a new set of protocols including http, URL, and html. It was these protocols that created the interface for today's World Wide Web (WWW).

The WWW concept was designed in **1989** by Tim Berners-Lee and scientists at CERN (Geneva), who were interested in making it easier to retrieve research documentation. A year later Tim Berners-Lee had developed a "browser/editor" program and had coined the name "World Wide Web" as a name for the program.

In **1991**, the World Wide Web was released to the public – the Internet was commercialised. The Internet is now available to everyone who owns a computer and has a phone line connected to a network.

The next step was to design an improved "browser"; a software allowing reading of HTML documents, activated by a click with the "mouse". In **1993** the first mainstream Web browser software, Mosaic, was introduced.

Thanks to the popularity of the web, the use of the Internet exploded after 1990, forcing the U.S. Government to transfer administration to private organisations starting in **1995** - four years after the Internet's commercialisation [105].

The Internet has resulted in an explosion of Web-based e-businesses and provides now access to electronic commerce transactions to millions of consumers and businesses. However, the realisation of the electronic commerce process is very difficult without an appropriate system for electronic payment. The development of practices for ensuring the security, audit ability, and non-repudiation of transactions that are well established in the paper-based world has not kept pace in the digital world. As the conventional payment instruments do not fit with requirements for improving the commerce process, new electronic payment systems should be developed to satisfy all requirements of electronic commerce. These *Internet-based electronic payment systems* are Web-based applications where payment for products and services are handled through a Web browser interface. However, one of the major inhibitors for e-commerce on the Internet is security and privacy issues. Subsequently, the acceptance of Internet-based electronic payment systems is dependent on the security measures that are offered to support these payment systems. The original intention of the Internet was for research and sharing of information, mainly by providing easy accessibility, not for electronic commerce. Thus, openness was the focus, and not security.

1.2 The Research Dimensions

1.2.1 The Research Problem

As the Internet is now being seen by many organisations as an efficient means to reach potential customers, **electronic commerce** and **information security** are growing areas of concern to user communities.

To date, most commerce on the Internet consists of the interactive dissemination of "advertising material" through the World Wide Web home pages, whereas the actual purchase of the product still occurs outside the network. Nevertheless, more and more commercial transactions are seen on the Internet. Several pilots have appeared on the Internet to support electronic purchases. While electronic transactions have reduced costs and improved efficiency over more traditional paper-based methods, they bring along increased security vulnerabilities, such as, interception, tracking or attack. These security vulnerabilities can have a great impact on the acceptance of various payment systems.

For electronic commerce to expand and electronic payment systems to gain acceptance by the public an improved security technology is needed to ensure accountability, information integrity and information privacy. Without the presence of a secure payment service and a well-developed security policy it is difficult to see how any electronic age could survive over an open network. If these payment systems are not secure, their acceptance by the public will be minimal.

The questions that will be addressed by this research are:

1) **What are the most commonly used payment systems?**
2) **Which security techniques exist up to date?**
3) **Can the electronic payment systems compensate for the conventional payment systems?**

In conclusion, this research problem is two-fold – promoting the design of secure electronic payment systems in order to assist the growth of electronic transactions, and analysing the security measures available for these electronic payment systems.

1.2.2 The Research Objectives and Benefits

The aim of this research is reviewing the traditional and electronic payment systems offered, examining the current existing security techniques, trying to make the Internet more secure and then evaluate how these security techniques are applied to both the conventional and electronic payment systems. A comparison between the various electronic payment systems, according to some evaluation criteria, will be drawn, in order to estimate which payment system is the best. Furthermore, finding answers to the three research questions will be addressed.

1.2.3 The Research Design, Instrument and Sample

Traditional payment systems are in use for years to conduct traditional commerce. Although these payment systems have a great acceptance level, they are not appropriate for commerce on the Internet. As a result, electronic payment systems are evolving in order to conduct electronic commerce on the Internet.

To estimate whether the traditional payment systems will be outdated in future, the three traditional payment systems (cash, cheque and credit cards) and the electronic payment systems (electronic cash, debit and credit cards, electronic wallets, smart cards and customer accounts) will compose the research sample. Using heuristic evaluation as the research instrument, these payment systems are analysed specifically according to their security aspects offered. Furthermore, evaluation criteria, such as, status and milestones, availability (access), convenience, security, support of micropayments and merchant risks involved, are used as instruments to compare the electronic payment systems with each other, and to be able to assign a score (out of 10) to them.

1.2.4 Data Collection and Analysis

The main source for the primary data collection consisted of explaining the various payment systems and finding arguments why security is important for payment systems, especially for electronic payment systems. Known characteristics and restrictions of security on traditional and electronic payment systems were captured in order to identify the strengths and weaknesses of each payment system. Secondary data collection consisted of printed literature on the Internet, electronic commerce, traditional and electronic payment systems, and security on the Internet. These sources were supplemented with applicable Internet-based resources.

1.3 The Scope

The examination of **security** and **electronic payment systems** has formed the basis for this research, whereas the security issue discussion is restricted to the application level only. Network access layer security, transport layer security, web server security, Internet layer security, database security, and legal and ethical issues in computer security are not within the scope of this paper. Network options (such as, access connectivity) available to e-commerce players are also excluded in the discussion about security.

The text covers a discussion of the important electronic commerce concepts, various traditional payment systems (excluding giro and wire transfer) and electronic payment systems. The various electronic payment systems are grouped into electronic cash, electronic wallets, micropayment systems, smart cards and credit and debit cards. Only the major electronic payment systems in each of these categories will be discussed within this paper. The electronic payment systems are then compared according to important evaluation criteria:

1) Status and milestones
2) Availability (access)
3) Convenience

4) Security
5) Support of micropayments
6) Merchant risks involved

The fundamental architectures that support electronic commerce applications are not explored in this text. Companies are not provided with guidelines or design issues on how to "get started with e-commerce". Open legal issues, such as, Internet tax policies, domain name disputes and inappropriate web linking practices, and technical and cultural issues do surely have a great impact on e-commerce and electronic payment systems, but are not examined in this context.

The text argues that the prime motivation for deploying electronic payment systems is making them secure and takes into account *security issues* and *concepts* and *security mechanisms*. Among some others, the following security mechanisms are identified: cryptography, encryption, digital signatures, digital certificates, the SET protocol and firewalls.

The legal impact for anonymous electronic payment systems is not evaluated. Other legal and taxation issues threatening the growth of electronic commerce and the technological infrastructure for electronic payment systems are not included in this research.

1.4 Solution Approach

The study "Internet-based Electronic Payment Systems" will take the following solution approach. First, an in-depth literature study, covering categories, such as, the history of the Internet, electronic commerce, security, traditional payment systems and electronic payment systems, is conducted. In order to conduct electronic commerce, electronic payment systems are needed. As a result of this, important issues related to electronic commerce are addressed to provide a general understanding of where the electronic payment systems will fit in. The payment systems and security techniques that exist today

are discussed in greater detail, highlighting the most important characteristics. This is followed by looking how secure the existing payment systems are and what security mechanism is provided by them. On a last note, the applicability of each electronic payment system is accessed, using evaluation criteria, in order to determine whether electronic payment systems will compensate for the traditional payment systems.

1.5 Synopsis

This thesis has been written to be read sequentially, and is presented in eight chapters.

Chapter 1. Introduction and Overview. This is the current chapter and includes an overview of all the eight chapters that constitute the body of this dissertation. The research problem, its aims, importance and benefits, the research instrument as well as the scope and solution approach are described. Furthermore, as electronic commerce has evolved as a result of the Internet, the history of the Internet and the movements that have led up to the emergence of e-commerce as a potent force, are addressed.

Chapter 2. Fundamental Concepts. This chapter starts the journey by exploring the very basic concepts that will form the framework for this paper: Internet, electronic commerce and payment systems.

Chapter 3. Overview of Electronic Commerce. Here the important issues related to electronic commerce are examined in order to provide an overview of why electronic payment systems are needed for electronic commerce. Included is a summary of the benefits of electronic commerce for both the business and the user, followed by a discussion of trust and dangers and other important issues in electronic commerce

Chapter 4. Security Aspects. Internet security is the most cited concern about not using electronic commerce. Corporate data is at risk when exposed to the Internet and therefore, security is needed in order for the electronic age to survive. Parties involved in

a transaction need to be assured that only *authenticated* parties and payment mechanisms are involved in the exchange, and that they exchange only those items for which they are *authorised.* At the same time the privacy and anonymity of the parties must be protected. This chapter highlights the electronic commerce security risks and threats, followed by the current technologies available to mitigate these risks. Current technologies include encryption, user authentication and authorisation, firewalls, and private networks.

Chapter 5. Traditional Payment Systems. Conventional payment systems are here to stay! Although more and more electronic payment systems exist, the convenience offered by traditional payment systems for physical transactions will always be unmatched. This is due to their widespread acceptance and high degree of relative security. Cash, cheques and credit cards are discussed as the conventional payment systems, excluding giro and wire transfer.

Chapter 6. Electronic Payment Systems. The most fundamental view of e-commerce for a business is effective interaction with customers and business partners. That is why electronic payments are an integral part of e-commerce. Chapter 6 contains/includes an overview of the various electronic payment systems used on the Internet.

Chapter 7. Traditional Payment Methods versus New Internet "Money". The sense of acceptance by consumers that all conventional payment systems have generated over time is very high. The electronic payment systems will only gain the same acceptance if they offer security and protection against fraud and wrongful manipulation. The way traditional payment systems and electronic payment systems ensure security is discussed briefly in this chapter. Furthermore, the electronic payment systems are evaluated according to six evaluation criteria: status and milestones, availability (access), convenience, security, support of micropayments and merchant risks involved. Finally, the applicability of the electronic payment systems is discussed.

Chapter 8. Conclusion and Future Research. The answers to the three research questions are examined, taking into account the research objectives. An overview of the conclusion reached is presented and suggestions for future research are offered.

The text concludes with a comprehensive bibliography, followed by a glossary of terms that will assist the reader in clarifying concepts related to this paper. Following the glossary is a set of appendixes, covering some related topics of special interest to the reader.

1.6 Conclusion

For electronic commerce to succeed, it must be complemented with a *secure* payment system, i.e. a payment system that provides trust. The importance of security techniques for electronic payment systems in order to ensure further growth of electronic commerce is indisputable. If electronic payment systems were not secure consumers would be reluctant to make any purchase on the Internet. Customers of e-commerce need the confidence that their online transactions are secure. Although the conventional payment systems have not operated on the open network and are already widely accepted, security enforcement is necessary for both the conventional and electronic payment systems.

For this paper it is important to investigate which security technologies could make the Internet-based electronic payment systems become a foundation for e-commerce and an acceptable payment method for both consumers and businesses, respectively, if an when yes, which reasons exists, that could avoid this. In order to evaluate the security techniques needed for both payment systems, I will identify the key security requirements and techniques in order to evaluate the security achieved by the identified payment mechanisms. I will then identify the different types of payment mechanisms that are proposed on trial and used on the Internet

Chapter 2

Fundamental Concepts

2.1 Introduction

In this chapter "Fundamental Conceptions" an explanation and concept composing of various conceptions, which are of uttermost importance throughout this paper, follow.

2.2 The Internet as a Concept

The Internet is an international or *global network of interconnected computers* that all work together to share information. According to the official definition of the Webopaedia [169], the Internet is "a global network connecting millions of computers." Put differently, the Internet is a world-wide collection of networks and gateways around the world, using the TCP/IP suite of protocols to communicate with one another, i.e. allow communication to the network users. It is a medium, an infrastructure or a communication platform for the resources transfer through it.

The Federal Networking Council (FNC) agrees that the following language reflects their definition of the term "Internet" [133].

"Internet" refers to the global information system that --

(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;

(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and

(iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

To summarise what has already been mentioned in chapter one: the Internet began in the 1960s as a part of America's military defences and was a decentralised network called ARPANET, created by the Department of Defence in 1969, to facilitate communications in the event of a nuclear attack. Later other networks, including BITNET, Usenet, UUCP, and NSFnet, were connected to the ARPANET. As of 1998, the Internet has more than 100 million users world-wide. More than 100 countries are linked into exchanges of data, news and opinions. Today, the Internet is accessible by anyone with a proper computer and modem and an ordinary telephone line. Using these components it is possible to dial into the virtual world of the Internet, access the wealth of information and then disconnect once finished. All of this is possible at the cost of little more than a local call. *Internet Service Providers* (ISP's), such as, America Online, are the firms that make this temporary connection available to individual users and small firms. They establish permanent connections into the Internet and then rent this connection to smaller users on a dial-up basis.

One of the greatest things about the Internet is that once a person is connected, he/she can tap into the millions upon millions of bits of information that lie on computers and databases around the world. All this information is stored on the World Wide Web. This of course explains why the Internet is also called the World Wide Web, or Web or *WWW*.

At the heart of the Internet is a backbone of high-speed data communication lines between major nodes or host computers, consisting of thousands of commercial, government, educational and other computer systems that route data and messages. One or more Internet nodes can go offline without endangering the Internet as a whole or causing communications on the Internet to stop, because no single computer or network controls it.[1]

Unlike online services, which are centrally controlled, the Internet is decentralised by design. Each Internet computer trying to access the information available on the Internet

[1] Copyright Microsoft press, Internet WWW page at URL: http://findmybusinessat.com/wde/info/define_internet.htm

is considered as an independent host of the Internet. At the same time any computer that is able to go online, is part of the Internet!

Currently, the Internet offers a range of services to users, such as, browsing the web, chat and instant messaging, e-mail, newsgroups, search of certain information and purchasing or shopping.

As there is sometimes a lot of confusion regarding the terms Internet, Intranet and extranet, Intranet and extranet will also be defined here. An **Intranet** is a private network that is based on TCP/IP protocols belonging to an organisation and accessible only by the organisation's members, employees or "outsiders" with authorisation. Like the Internet, the Intranet is also used to share information that needs to be quickly and easily disseminated, such as, in-house newsletters, company policies and phone lists, etc. In actual fact, any information that needs to be sent within an organisation can be sent via its Intranet. An Intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an Intranet prevents unauthorised access from outsiders' [128]. The Intranet can be viewed as a mini version of the Internet.

When a corporation opens up portions of its Intranet to authorised users (such as, suppliers, business partners and customers) outside the corporation an **extranet** exists. Extranet users are given a login and password, which tells the computer specifically what information they are entitled to view. When a company wants their customers to place their own orders they should make use of the extranet.

2.3 Electronic Commerce as a Concept

Thomas O'Daniel [78] defines Electronic Commerce (or e-commerce) based on the perspective it is looked at:

a. The "*economical perspective*" addresses the desire of buyers and sellers to cut their costs, while increasing the speed of their service and the quality of goods.

b. The "*management perspective*" applies electronic commerce technology in order to achieve automation in business transactions and workflow.
c. The "*marketing perspective*" looks at electronic commerce as a new vehicle for providing product information to a target market through advertising, promotion and publicity.
d. From the "*technology perspective*", electronic commerce means the delivery of information, products, services and payments via computer networks.

Combining these perspectives into a business plan means, to set up the appropriate e-business system, in order to earn more money for the company.

The following definition of electronic commerce (shortened e-commerce) will form the framework for the material of this text: "*The buying and selling of information, goods and services over the Internet's World Wide Web. This encompasses all electronically conducted business activities, operations and transaction processing, which include: the deliver of the product, order processing, billing, credit card payment, electronic cash transactions and customer support.*" For the purpose of this paper only the payment mechanism involved in e-commerce transactions will be considered.

E-commerce encompasses all ranges of transactions, such as, business-to-business, customer-to-business and intra-business, all relying on each other for supplies, distribution, services and technology. The main methods of e-commerce remain the Internet and the World Wide Web, but the use of email, fax and telephone orders are also prevalent. The Lotus Development Corporation revealed the following definition. Electronic commerce is a range of applications that extend the core business activities of the enterprise into a virtual electronic community. The electronic commerce process does not begin and end with the sale. Extended enterprise applications support a variety of functions that facilitate the movement of information and communication among members of the enterprise-centred community [65].

E-commerce technically implies electronic devices and complicated networks to be able to work together to complete commerce-related tasks [29]. Electronic commerce is

therefore, using the Internet, Intranets, extranets and private networks (referred to as communication networks) for doing business, whereas doing business covers the buying and selling activities of goods and services.

According to Keen [48, page xvii], e-commerce is defined as the "systematic design of trusted relationships." Using e-commerce there is no face-to-face contact and a lot of uncertainties exist. To avoid these risks, trust must be established. The challenge for e-commerce is that most of the trust assumptions that paper commerce takes for granted are not built up in e-commerce and cannot be taken for granted.

Some people and businesses use the term **electronic business** (or e-businesses) when talking about e-commerce in a broader sense, referring to business-to-business electronic commerce. It implies performing day-to-day business transactions, using combinations of e-commerce technologies. Electronic business therefore, also includes the exchange of information not directly related to the buying and selling of goods. **Internet commerce** is used for electronic commerce that specifically uses the Internet or the Web as its data transmission medium [92]. In this paper, the term e-commerce instead of e-business will be used.

From the above it is clear that there are several variations for the definition e-commerce and no single, globally accepted definition exists. However, no matter what the definition, e-commerce is becoming an important way for processing transactions between buyers, sellers and suppliers all around the world.

2.3.1 Trust

Trust is the building block or foundation for both secure commerce and secure e-commerce. Trust, especially among the trading partners in electronic commerce reinforces the prospect of continuity in a relationship and a commitment to extend an inter-organisation relationship. It implies that the trading partners are dependable and follow their promises, thus developing high levels of co-operation, which will in turn

reinforce trust [73], [22]. Trust requires face-to-face interaction, whereas this interaction is normally not present in electronic commerce. Therefore, trust is even more important in electronic commerce. As Handy [39] already notes, "the more virtual the organisation, the more its people need to meet in person." In virtual form trust is the primary means of social controls and co-ordination [72].

2.4 Payment Systems as a Concept

Payment, today, is a financial exchange between a customer and a business entity. In the earlier days payment implied exchange of goods and services between two parties through barter. [2] Cash as a medium of trade came into service during the first millennium B.C. The different varieties and forms of cash that exist today, such as, credit cards, debit cards, stored-value cards, money orders and cheques, were "born" only in the 20th century [105].

A payment system or strategic information system forms the foundation for the financial sector and is an *agreed upon way* to transfer value between a buyer and a seller in a transaction. The *purpose* of the payment system is to provide an infrastructure for transferring money from one entity in the economy to another.

Payment systems are distinguished by the **payment mechanisms** used to transfer value in an exchange of goods or services. They enable payment mechanisms to be used as mediums of exchange. Currency or money, cheques, credit and debit cards are all various types of payment system mechanisms.

[2] Barter is still common world-wide. It is estimated that 40% of Russia's business is done through barter.

Money as a payment mechanism in the payment system is a medium that people are willing to accept for the goods, securities and services that they sell [96]. Money serves three purposes [162]:

1. Money is a medium of exchange
2. Money is a standard of value for different goods and services
3. Money functions as a store of value and can be saved and used in the future

In order to fulfil the above mentioned purposes money must be durable, not easily counterfeit and, of course, widely acceptable. People will only accept a certain payment mechanism, if they know it is trusted as the medium of exchange and they can use it again as a method of exchange or store it as value.

Payment systems play a major role in the conduct of a country's monetary policy and support the growth of financial transaction. Firms in different economic sectors use the payment system to transfer funds and to provide competitive financial service [51]. The payment cycle involves the transfer of funds that differ in volume and value. A retail payment system or small-value funds transfer system manages high-volume and low-value transactions. Whereas the wholesale payment system or large-value funds transfer system covers low-volume, high value transactions. A model of a typical payment cycle is illustrated in Figure 2-1.

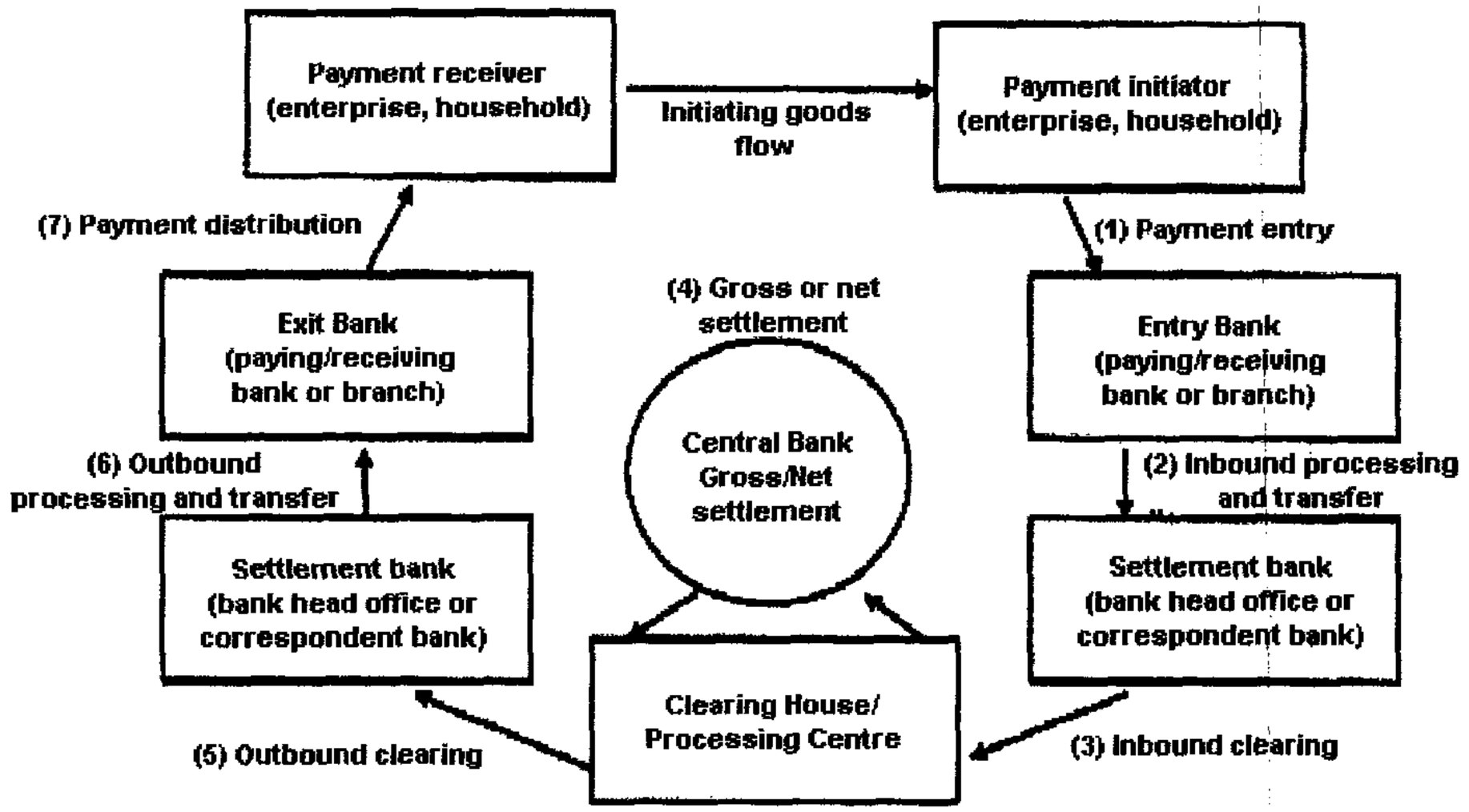


Figure 2-1 Model of a typical payment system [51]

The *goal* of an efficient payment system (whether traditional or electronically) is one that allows instant confirmation of a transaction, allows buyers and sellers to directly exchange the necessary information and value for consummating a transaction without third party confirmation, and does so within a secure environment [84].

Payment systems have been used to support traditional commerce and will also be used to support electronic commerce. No matter what payment method is used, whether cash or credit, a certain level of trust needs to be present for that payment method to be accepted as a payment tool. The whole structure of traditional money is built on faith, just as electronic money will have to be.

Payment systems are to economic activity what roads are to traffic – necessary but typically taken for granted, until they cause an accident or bottleneck. Security of electronic payment systems is currently one of the greatest concerns.

2.4.1 Micropayments

The rise of online content as a commercial product requires new forms of payment like, micropayment. Micropayments, sometimes called millicent- or microtransactions, are transactions that range from 1/10 of a cent to $10.00 and up, with varying limits being set by the micropayment system developer [136]. A **micropayment system** is needed for pricing of these microproducts and microbundles and for handling small amounts of money: a part of a cent. The digital coin systems are a suitable approach to pay for these microtransactions.

Traditional payment methods make sub-dollar transactions expensive due to their high administrative overhead. The administrative overhead tends to be more expensive than the actual product.

Vendors should use the micropayment systems to sell low-value services or information. Low-value transactions include the sale of digital content (e.g. information, such as, one article from a daily newspaper), download of web content, renting software by the hour etc. To achieve a low per-transaction cost, communication traffic costs must be cheap, per-transaction overhead must be low, no expensive cryptographic techniques should be used and a high processing rate is required.

Some sources differentiate between micropayments and small payments, where small payments start from at least 0.1 USD. In this paper, the term "micropayments", as defined above will be used and no differentiation will be made.

2.4.2 Macropayments

Macropayments are transactions that start at about 10 USD. According to O'Mahony, Peirce and Tewari [79, page 193], a macropayment is "a transaction capable of handling payments worth several dollars or more." The traditional payment systems like credit cards and cheques are examples of macropayments. The parties involved in such a

transaction will be interested in being authenticated in order to protect themselves from fraud. Any information exchange must be secure and confidential to avoid eavesdroppers gaining access to details of the transaction. Finally, payment must be assured via online verification.

2.5 Conclusion

Throughout this chapter, when reference is made to the concepts: Internet, electronic commerce, payment systems, micropayments and macropayments, the above definitions and descriptions will apply.

Chapter 3

Overview of Electronic Commerce

There are quantitative changes so profound that they become qualitative. For example, e-mail is much the same as regular mail but faster. However, it is so much faster that it has the power to reshape companies, create communities, eliminate geography and revitalise the art of letter writing in a generation which had been thought of have been rendered incapable of it by television. That is a qualitative change. Now think of Internet electronic commerce as the e-mail equivalent of traditional commerce's surface post.

Jeff Bozos, founder of Amazon.com [105].

3.1 Introduction

Thanks to the technology of the web browser, the Internet has resulted in an explosion of web-based e-businesses[1] causing fundamental changes in traditional business processes. Electronic commerce differs from traditional commerce in the way information is exchanged and processed. Historically, transactional information was exchanged through direct, personal contact or by using the phone or postal systems. With electronic commerce some form of electronic processing is used for the exchange of value-information, through a digital communication network, computer system, or any other electronic media. This chapter presents the various activities encompassed by electronic commerce and the role of the Internet as enabler of electronic commerce. Advantages and disadvantages, trust and dangers and other primary issues relating to electronic commerce are summarised.

[1] See Appendix F for a list of successful e-commerce sites.

3.2 What is Electronic Commerce?

E-commerce links companies, customers, suppliers, employees and distributors, and has changed the way companies do business. In some cases it replaces non-electric ways of product and service delivery, as well as customer involvement; in other cases it supplements them. A transaction occurs when a product or service is transferred over an interface linking the manufacturer (server) and the customer (client). E-commerce transactions are controlled electronically from ordering to delivery and can involve individuals, business firms, non-profitable organisations and governmental entities as both buyers and sellers.

Electronic commerce utilises *different technologies* and *forms* when sending electronic data messages between enterprises. Examples are electronic banking and trading, electronic funds transfer (EFT, also called wire transfer), electronic data interchange (EDI), electronic mail (e-mail), facsimile transfer, electronic cataloguing, video conferences, multimedia communications and other forms. These different forms of electronic commerce are redefining the nature of markets world-wide. The venue for transacting a business (marketplace) has moved into the cyberspace markets. According to Shim [95, page 80], e-commerce can be divided into:

- E-tailing or virtual storefront sites with online catalogues, sometimes gathered into a virtual "mall".
- Gathering and use of demographic data through Web contacts.
- Electronic Data Interchange (EDI), the business-to-business exchange of data.
- E-mail and fax media used for reaching prospects and established customers.
- Business-to-business buying and selling.
- Security of business transaction.

Apart from the e-commerce categories, the following *business models* can be differentiated:

- E-shops, E-malls, E-auctions, E-procurement
- Virtual communities

- Third-party marketplaces
- Value-chain integrators
- Value-chain service providers
- Information brokerage

Many design issues, such as, electronic catalogues (i.e. product pricing and product information), advertising a product or service, language, security, paying for a product or service, and trade or taxation laws need to be considered when creating an e-commerce application.

3.3 Why Businesses are attracted by Electronic Commerce

Businesses and individuals, using electronic commerce, have been able to create new products and services, create a new sales channel for existing products, improve purchasing and supply activities, identify new customers, reduce transaction costs and administer some other activities more efficiently. However, the main attraction points of e-commerce can be identified as:

a) *The market penetration is tremendous.*

   Recent statistics indicate the tremendous growth of Internet users. In the near future, it can be assumed that every household will be online.[2]

b) *24 hours a day x 7 days a week availability.*

   The Internet and the electronic Web page of any online store are available 24 hours every day. They grant immediate and easy access to the assortment of the store, without any restrictions on weekends or through opening hours.

c) *Direct savings.*

   By using a public shared infrastructure, such as, the Internet, marketing, distribution and customer service costs can be drastically reduced.

[2] See Appendix B for recent statistics on the number of Internet users.

d) *E-commerce is world-wide, direct and everywhere.*

The Internet works on a global basis, reaching all corners of the World. A firm can use electronic commerce to reach narrow market segments that are widely scattered geographically. There are no physical borders, time zones leading to time delays, language differences or cultural barriers for accessing a web page. However, for deliveries there may be restrictions.

e) *Multimedia.*

Multimedia tools can help gaining a competitive edge in information provision during buying and selling. This will provide entirely new opportunities in consultancy, design and entertainment in combination with inter-activity and networking.

The following *shortcomings* of doing business on the Internet are one of the major concerns for a business and his customers:

a) Information security concerns, for example, hackers can get access to any personal information. Data travelling on the WWW can travel through non-trusted systems, providing no integrity guarantee.
b) Some organisations, conducting business on the web, are sometimes non-trusted, as they not necessarily have an existence outside the electronic environment [4].
c) Credit card fraud, which leads to unsecured transactions.

3.4 The Business Processes

The sales activities that companies undertake when engaging in any kind of business play a very important role in e-commerce. The various stages in the shopping process of e-commerce can be summarised as customer care, search, purchase, delivery and post-purchase. For most of these stages specific software or components are being developed. Auctionware, catalogues, customer relationship software, shopping charts, product tracking are examples thereof.

The e-commerce life-cycle model is presented in Figure 3-1. The e-commerce cycle for the seller is making customers aware that a product or service exists, i.e. providing information about the product or service, finding the customer, filing the order and providing post-sale customer support and service. Customers usually pay for items with a credit card or digital cash (which will be discussed later). Purchasing cards and electronic payment systems will need to be integrated with business processes. The e-commerce cycle for the buyer is identifying a need, finding a source that will satisfy the identified need, evaluating the good or service for possible acquisition, purchasing the item and using the item. From the buyer-seller perspective electronic commerce can be used in all phases of a commerce transaction.

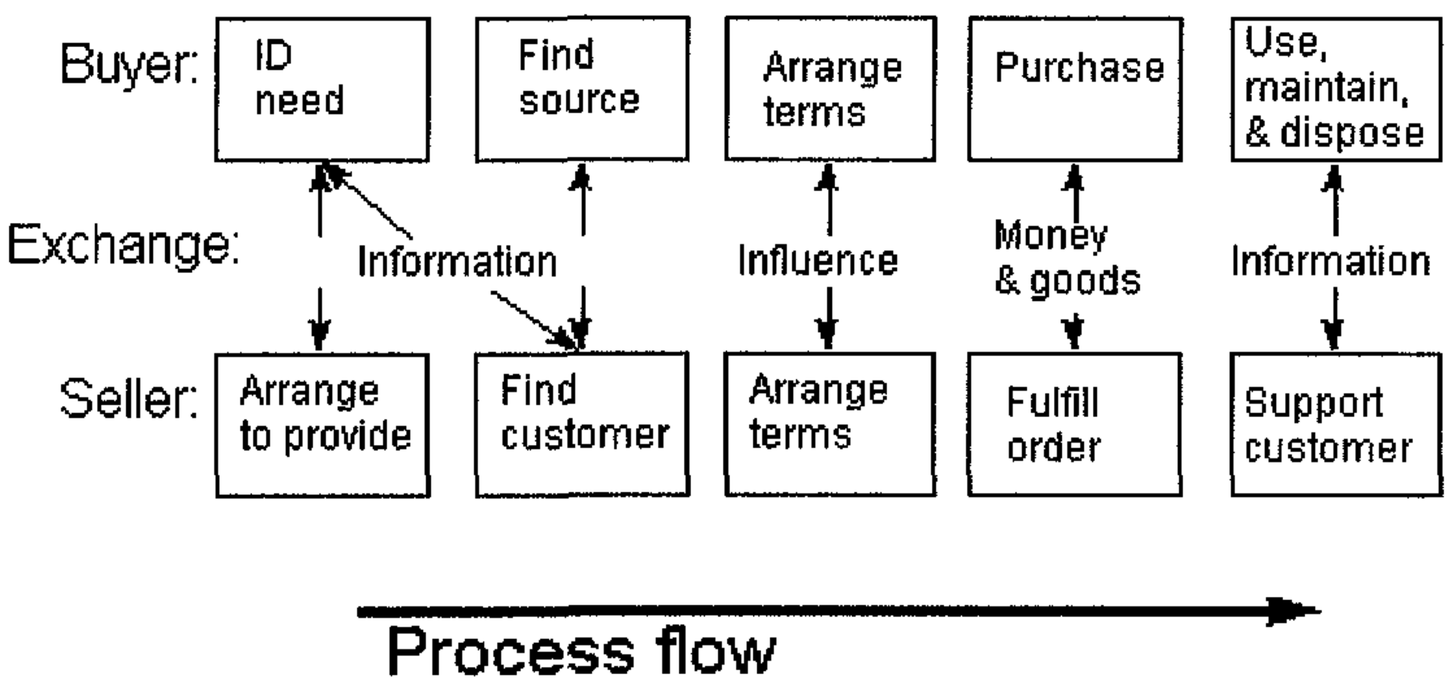


Figure 3-1 Electronic commerce model [76]

Web pages serve as sales assistants providing product information. When a customer enquires about a product, the databases are queried, the best prices are provided and delivery is scheduled as soon as the order is placed. The virtual shopping basket allows the shoppers to combine their purchases from a site.

Electronic commerce can automate the business processes within a company. This permits faster marketing and delivery of goods and services to consumers. Furthermore, using electronic commerce the communications time between negotiating parties can be reduced, leading to faster information sharing between suppliers and customers.

3.5. Important Issues related to Electronic Commerce

In order to understand electronic commerce it is of importance to understand some important issues related to electronic commerce.

3.5.1 Cybermediaries

Disintermediation refers to the removal of an established intermediary by replacement of a direct connection between the parties [105]. The Web was identified as a source of disintermediation effects. However, e-commerce provides new intermediation opportunities, allowing intermediaries to expand in importance as transaction and information volume increase.

Cybermediaries, also called network-base intermediaries, are the new generation of the well-known traditional intermediaries. They are organisations that play a fundamental role in encouraging, promoting and facilitating business-to-business relationships. Hence, they perform the mediating tasks in the world of electronic commerce by relying on information and communication technology. The most obvious characteristics of cybermediaries are that they appear to facilitate complete Internet transactions, end to end, without assuming ownership of the product.

The main purpose of cybermediaries is bringing together buyers and sellers, by providing information and distributing goods and services. Buyers, however, benefit explicitly from functions, such as, assistance in search and evaluation concerning price and quality needs assessment, bargaining discounts, notification of information changes and product matching. Intermediary functions that benefit sellers include creation and dissemination of product information, creation of product awareness, processing of suppliers' responses to queries, purchase influence, and providing customer information. Therefore, intermediaries must provide a bundle of services that match user demand and provider's supply in the best possible way.

Traditional intermediary services, which range from a variety of explicit and implicit services for their customers, are not replaced by cybermediary services as they have different qualities and abilities. The services provided by traditional intermediaries are just likely to change significantly. Some skills may no longer be needed in electronic commerce while others may have additional value. Network-based services may, for example, do a particularly good job in facilitating product search, but are less well equipped to offer product distribution [89]. The major types of cybermediaries emerged are [95]:

- Certificate authorities issue certificates to individuals and WWW servers ensuring authentication.
- Financial intermediaries, such as, Quicken, banking institute, offers online banking. These intermediaries use systems from First Virtual and CyberCash to absorb some money risk flaws and to protect against merchant fraud.
- Intermediaries in the area of customer acquisition, e.g. the OnSale's site create an auction environment for computer equipment.
- Information directory providers, such as, Yahoo, are service providers in the information phase of a market transaction. These sites help identify products, services, articles and other Web sites. By using these portal sites, a customer can identify product and service providers and acquire information on the quality and cost of a specific item.
- Web service providers, provide new places for producing and manipulating web data. These type of intermediaries operate on web data as soon as the request is sent from the browser, passes through firewalls, and as the document is returned to the browser, extending the content computation beyond the server.
- Information access providers, such as, Microsoft Explorer, provide access to the Web and Web-site hosting services on a subscription basis.
- Network access providers, such as, America Online.
- Intelligent agents, also called just agents, are software programs that perform information searches on behalf of a person or entity. Anderson Consulting has created the intelligent site known as BargainFinder for research purposes.

A great deal of online intermediary functions are associated with the financial sector. These financial intermediaries or economic agents, stand between the parties of a contract, performing functions necessary to fulfil the contract. They include the merchant server, payment-acquiring bank, issuing bank, credit card processor, third party processor, brokers and traders. Financial intermediaries are responsible for transaction management, inventory, accounting, authorisation and settlement. Intermediaries guide customers by providing the sites that allow buyers and sellers to transact business, make bids, or exchange information with the intermediaries facilitating the transaction.

Privately negotiated transactions lead to limitations, such as, lack of privacy, pricing inefficiencies, incomplete information, search costs and contracting risk. Intermediaries, whether online or offline may remove these limitations. They can secure a desirable price for a product, provide product information not only from the product provider, maintain databases of user and provider preferences and ensure anonymity of both the seller and the buyer. At the same time, intermediaries help to establish a great deal of *trust* between trading partners. Buyers have no guarantee that the information presented on the Internet is valid and that the payment systems being used are reliable. Users, on the other hand, cannot distinguish the insecure Internet environments from the secure Internet environments. Intermediaries will ensure the integrity required for completion of any transaction.

It is therefore clear that new virtual communities of intermediaries have formed, and they will continue to form, as a result of the introduction of e-commerce.

3.5.2 Marketspace

E-business systems are offering customers choices to search for a company. Every company can decide which type of channel to provide for their customers. Transaction channels, which are available to reach customers, include phone, fax, branded storefronts, one-to-one computer (point-to-point) and the marketspace.

A marketspace (sometimes called online marketplace) is a new term used to describe the transition from traditional markets, defined by physical location, to a virtual location where products and services exist as digital information and can be delivered through information-based channels. This transaction channel, bringing together supply and demand as well as generating a contract between the supplier and the customer, provides another way for the customer to place orders and to enable one-step business transactions.

The marketspace is not simply an online marketing brochure, it becomes a gathering place, a place providing trusted source of information to get answers to questions, and a secure place to conduct business. Directory and search services, a targeted list of links to other information sources on the Internet, access to articles and publications, discussion and chat groups, and classified advertising are all functions provided by a marketspace. Its mission is to engineer business collaboration across enterprises via the Internet.

In a situation where a company has already established an own business portal, the marketplace would function as a *substitute* for this established portal. A customer could then use the marketplace or the company's portal to place an order.

How a marketspace works, depends on the marketspace chosen. In most of the cases, however, a buyer creates an order and the marketspace routes this information to the seller. The seller, and not the buyer, pays a transaction fee to the marketplace. "Elemica"[3] is one of the premier, neutral e-marketplaces for the chemical industry globally and has established direct contact with 22 investors. Elemica was formed in August 2000, conducting the first transaction in January 2001. If sellers are connected to the same online marketplace, a buyer can place an order on one browser rather than using, for example, three different URL's, i.e. for each different seller one URL.

Electronic commerce conducted through a marketspace offers **advantages** to both buyers and suppliers. For buyers, the marketspace will provide access to a greater number of

[3] Elemica's Homepage is found at URL: http://www.elemica.com.

sellers. The biggest benefit of a marketspace to sellers is providing them with access to a great number of buyers, i.e. to the market. Due to the size and disorganisation of the Internet it is very difficult for customers to find a site they want to purchase from. The marketspace addresses this problem in several ways [168]:

- Customers are informed about the marketspace presence.
- Community and communication elements offered by a marketspace increase the customer's trust level.
- A streamlined business process flow with one-step business is provided. As the marketspace represents an aggregation of suppliers, customers do not need to visit a dozen of sites to purchase. Instead, they can browse the member merchant web sites and procure products and services simply by accessing one site.

Although the marketspace is becoming more and more attractive for suppliers, there are still some **disadvantages** they have to consider:

- Customers and suppliers are still resistant to this new channel and not always interested.
- No traffic ramp-up (meaning no revenue) exists for suppliers.
- Developing a marketspace requires significant investment, but currently no funding is available for online marketplacess – not from the bank, suppliers and customers.

3.5.2.1 Categorisation of Marketspaces

A convention has arisen that analysis marketspaces into categories, depending on the nature of the buyer and of the seller.

The four *categories* of e-commerce identified are:

B2B: Business-to-Business

B2C: Business-to-Consumers

C2C: Consumer-to-Consumer

B2A: Business-to-Authorities

3.5.3 Finance on the Web

Electronic business transactions can only be successful if payment between buyers and sellers can occur in a simple, universally accepted, safe and cheap way. The payment is necessary for a compensation of goods and services, including things, such as, copyright material, database searches and consumption of system resources [126].

Various electronic payment systems have been proposed. Some of them are based on traditional mechanisms (e.g. credit cards) while others rely on new designs, such as, electronic money. Internet payment companies, such as, CyberCash, First Virtual, OpenMarket and CheckFree provide merchants with Internet payment systems for establishing or expanding their Web presence, and are trying to make their systems as secure as possible. Consumers can now use credit cards, digital cash, electronic cheques, electronic wallets and micro-cash to pay for their electronic transactions.

Electronic commerce will play a dominant role in shaping the finance on the web. Businesses are already changing face of business. Visa and MasterCard have formed the entity called SET (Secure Electronic Transaction) LLC [65]. The SET standard was designed to provide a higher level of security for payment card transactions over the Internet. Mondex International [143] has introduced "Mondex" around the world as an alternative to notes and coins. Finally, banks will have to change their face of business as they are now faced with digital currency and electronic cheques.

3.6 Trust in Electronic Commerce

Trust and security are the main building blocks for e-commerce. The trust in real world transactions is provided through a physical meeting and/or references. Lack of such trust is often seen as the most signification barrier for e-commerce.

As dishonest/illegitimate electronic commerce transactions can result in legal actions it is of uttermost importance to verify that the parties in a transaction are really the people they pretend to be. There are many different ways in which e-commerce can be structured so as to achieve this sufficient trust between buyer and seller. A lot of effort is being invested in developing trust through "**authentication**", and there are several different ways in which authentication can help.

One approach is **value authentication**, which refers to checking that the banknote is not forged. On the Internet, forgery of digital money is feasible, but not if the people minting it use the electronic equivalents of complex visual designs, watermarks and hidden metallic strips.

Another form of authentication is called **eligibility authentication**. This means checking that the buyer the company is dealing with, in reality has a particular capability he/she is claiming. For example, does the person have a license to sell those kinds of goods? There is a need for electronic equivalents of, for example, membership-cards, in order to establish confidence.

A further approach is **person authentication**. This involves ensuring that the other person is who they claim themselves to be. These various authentication techniques are based on cryptography. The particular application of cryptography that assists most in authentication is the technology called "*digital signatures*". These are long numbers that are able to demonstrate that a particular message has come from a particular person or organisation.

Finally, the **biometrics** technology[4] is being used more and more as an authentication mechanism. Biometrics requires measures of some physically unique characteristics of an individual's body to be used for identification [24]. Fingerprints are currently one of the biometric systems commonly in use. Other biometric sources in use are voice

[4] See Appendix A for an overview of the current biometric authentication methods.

recognition, face recognition, signature recognition and eye scanning, with retina scans currently considered to be the most secure.

3.7 Dangers in Electronic Commerce

Unfortunately, e-commerce is prone to serious risks that result in some highly undesirable side effects. As already mentioned, in order to establish trust, people should identify themselves. At the same time, however, this trust could also create a danger for electronic commerce.

Most real-world transactions are undertaken by using cash, and most of those are anonymous. Even if the buyer and seller recognise one another, the identity is not recorded and stored for all time. Hence, any move towards "**identification**" as a requirement for electronic transactions would reverse a long history of anonymity, and would generate new trails of personal data that have never existed before. Moreover, these trails would be likely to be very intensive, i.e. to show a great deal about what each person is doing, and where they are, at every hour of the day. Even if most electronic commerce transactions remain anonymous, some will need to be identified.

For digital signatures to assist in establishing trust in electronic commerce, a public key will have to be reliably associated with a person. That person will need to present evidence of his/her identity to a certification authority (CA). The CA will then post a certificate, assuring, that particular public key is associated with an identified person, in an electronic public place. This is another identification, which might lead to discomfort.

Another danger is "**biometrics**". There are continuing attempts to use genetics as a basis for human identification, which would be likely to require the provision of body fluids or tissue. Proposals for the use of microchips as a means to identify humans have already been placed. This could take overhand if operators of ID schemes in companies and

government agencies will assume that these biometric measures should be stored in their databases as a reliable identification mechanism.

3.8 The Role of the Internet

The advent of the Internet, and all of its global sub-networks, enabled so many different forms of e-commerce utilities, all of which depend on a series of infrastructures, among them being the Internet. In summary, the Internet, as a communication infrastructure, is supporting the development of electronic commerce applications and at the same time fosters the growth of electronic commerce.[5] The role of the Internet in e-commerce can be summarised as follows:

a) *Makes the size of the company irrelevant*. Large and small companies have the same access to customers and can create the same kind of Internet presence.
b) *Makes the location of the company irrelevant*. Customers located anywhere can easily access the company's site. Every customer can be supported even those customers outside the geographic area. The zone and country does not play a role. The Internet is accessible twenty-four hours a day, seven days a week. Current staffing can be maintained while providing current and potential customers with extended hours of support and services. Customers will have access to the complete book line offerings.
c) *Increases feedback.* The company has instantaneous access to customers' responses and feedback when new marketing and pricing programs and new products are published on the web site.

Although the above points reflect some of the positive effects the Internet has on e-commerce, the reliance of e-commerce on the Internet brings some dangers or negative aspects with it. The Internet is often referred to as a non-trusted, distributed network. Consumers will do business with organisations they do not know, unaware whether they can trust them or not. On the other hand, it is also difficult for businesses to know that

[5] See Appendix C for the e-commerce growth in different regions.

customer A is really customer A or that the transmitted data has not been intercepted and modified [23]. Due to the distributed nature it is difficult to control security measures. Network congestion, leading to poor response times, will affect the performance of the e-commerce application and provides unreliable service to users. Last, but not least, users who do not have access to the Internet (usually the third world countries) will not be able to be involved in electronic transactions, reducing the growth and/or development in e-commerce to some extent.

3.9 Conclusion

The widespread infrastructure of the Internet along with the low-cost connectivity to the Internet offers sellers (i.e. businesses) a great opportunity to get involved in e-commerce. E-commerce is not just a technology but a very powerful *business channel* with promises for further development, forcing businesses to rethink or change their traditional way of conducting business, and impacting every aspect of the firm's value chain.

The primary *benefits* for companies are global presence, improved competitiveness, reduced cycle times and low costs, while consumers benefit from added convenience, access to information and price comparison. This chapter showed that electronic commerce involves more than just buying and selling over the Internet. Broader uses of e-commerce include electronic mail and messaging, fund transfers and payments, a way to provide information to customers (e.g. access to product brochures), a marketing tool (e.g. advertising and promotion of goods), a sales channel, and a support line. Apart from the e-commerce uses a lot of other areas are effected. Some of the general impacts of e-commerce are its effect on marketspaces and on intermediation. E-commerce systems replace some of the functions traditionally performed by intermediaries or information brokers, but at the same time allow for new forms of intermediaries, named cybermediaries. Finally, e-commerce allows for fund transfers and electronic payments between buyers and sellers.

The materialisation and success of e-commerce, however, depends on the security that is offered by any e-commerce system. Customers, as well as businesses, must be assured that business transactions conducted electronically are safe and secure. Businesses involved in e-commerce must be aware of all the security risks and threats associated with electronic transactions over the Internet. General business risks, such as, fraud, theft, destruction, corruption, interception, alteration and re-routing of corporate data, have made the comfort level over security found in e-commerce, not as strong as found in traditional commerce. Two major concerns of customers are transacting with false web sites posing as legitimate businesses and theft or misuse of information. All these security threats must be addressed in order to make the Internet a more reliable and *trusted medium* and at the same time protect online transactions. In this way, the risk of doing business electronically will be reduced and customers will *increase* their *confidence level* about e-commerce. Increasing the customer's confidence level normally implies higher levels of trust and trust is the basic building block for secure e-commerce.

Chapter 4

Security Aspects

Doing business electronically is increasing rapidly both for companies and for consumers. But without security and trust, there won't be a notable shift towards commercial and financial transactions on the Internet.

Erkki Liikanen, European commissioner responsible for the Enterprise and Information Society [43].

4.1 Introduction

While the Internet has provided businesses with an attractive commercial channel the dark side is that it is insecure as an "open systems", where there are no trusted gatekeepers to authenticated the identity of users entering the system. As information resources are placed over unsecured open networks, security and trust are a very important concern for today's information age and form the core to e-commerce. If electronic commerce continues to accelerate its volume without improvements in security, a great deal of commercial losses can be expected.

Absolute security is nearly impossible to achieve, but whether users are sending e-mail over the Internet or act as customers and engage in business they need to feel confident that their information or their transactions are not being altered. Consumers, conducting electronic transactions, want to be protected in the same way as when involved in traditional transactions.

Security is expected at two different levels:

- During the transfer of the information over the network
- When payment data is stored, i.e. protecting the systems

In reality, security is concerned with risk management [103], and trade-offs between accessibility and vulnerability. An organisation must estimate the cost for the different types of information and then decide what constitutes a reasonable cost to protect it.
Modification of data, whether accidental or intentional, is one of the main reasons why security needs to be enforced by businesses or individuals. To ensure computer security the computer resources (assets) must be protected from unauthorised access, use, modification or destruction. This chapter discusses the existing security threats and reviews the various reliable security methods and technologies that exist for a business to make any Internet transaction safe.

4.2 Security and the Net

Networks can be classified as local area networks (LANs) or wide area networks (WANs). Both these networks need security. Computer systems are becoming more dependent on networks and therefore, are more vulnerable to network attacks. A companies network resources must have controlled access, protecting them from everything originating from within the organisation (client-to-network) or the Internet (network-to-network). To secure the network, not only the telecommunication links must be secured but also the client's computer and the web server.

According to Barnett [6, page 14], a complete network security solution must provide the following control features:

a) Verify the identities of network users.
b) Encrypt data in transit between the client and gateway in order to secure the content of network traffic.
c) Optimise the use of registered IP addresses.
d) Detection and response mechanism to detect and respond to attacks in real-time.
e) Provide complete audit information.

Security is mostly compromised when access controls to network resources are improperly used. This means the controls are not necessarily weak but they are not properly configured. Hackers try to gain unauthorised access to a computer by finding bugs or misconfiguration problems in the web server that allow them to [65]:

- Gain access to confidential documents.
- Modify the system by executing commands on the server host machine.
- Gain information about the Web server's host machine, allowing them to break into the system.
- Launch denial-of-service attacks, by crashing or flooding the network or firewall and rendering the machine temporarily unusable.

4.2.1 Secured Internet

When the Internet was built, security considerations were not of great importance. Only after the Internet was opened to the public, especially for conducting electronic commerce, security is holding a great importance.

The Internet needs to be secured, as there are more and more aspects of crime on the information superhighway. These range from misrouting, transmission failure, illegal interception, theft or privacy of telecommunications services, electronic vandalism and terrorism, electronic funds transfer crime to money laundering. Internet attacks may include masquerades and interception, unauthorised use, service denial, disclosure of sensitive information or alteration of materials. Further examples of electronic threats are impostors, eavesdroppers, hackers and thieves.[1]

Any information moving through the global system of *interconnected computer networks* must be protected against risks that revolve around information privacy, integrity and availability. Whether the Internet is used for electronic mail or for shopping, it must be secured to avoid unauthorised access to messages and web sites. Using the Internet,

[1] See Appendix D for a further analysis of threats.

messages and files can be sent to staff, customers and vendors all over the world. How do you know that these e-mail messages or file transfers aren't being intercepted and being read on the way to their destination? As a result of these crimes the Internet should be protected from physical and electronic threats in order to become a trusted medium to carry transactions.

4.2.2 Secured Server and Browser

The server can be accessed from unauthorised users, most likely through the web server, any back-end programs or the Common Gateway Interface (CGI) programs. These entry points should therefore, be secured to avoid any security attacks.

A web server can run at various privilege levels. The higher the privilege levels set, the more unconstrained the access. The privilege levels are set for programs and system administrators, depending on the privilege level they need. Security settings should be set for automatic directory listings, File Transfer Protocol (FTP), and the file that holds the user-word and password. When unauthorised users gain access to the authorised users authentication information they can access the web server. In the same way they also can access a companies database, when the username/database pairs are stored in the database in a non-secure way. The CGI is a program used by web applications to connect users to databases. When the CGIs' actions involve printing a source code of the web server, it presents a security threat.

Secure browsers and servers are only designed to protect confidential information against network eavesdropping. Without system security on browser and server sides, confidential documents are vulnerable to interception.

4.2.3 Secured Communication Channel

The communication channel connects the clients and the server (the Internet). Messages travel from the source to the destination through a number of intermediate computers on

the network [92]. Communications security means that the data is being transmitted, while breakdowns, delays and disturbances are prevented. All unauthorised individuals should be prevented from tapping or modifying data transmission. Communications security should consider the following securities:

- Line security
- Transmission security
- Digital signature
- Cryptographic security
- Emission security
- Technical security

4.3 Security Risks and Threats

Today a number of security threats and risks exist, which can inflict various types of damage causing harm or loss to computing systems and to the electronic commerce environment. Misuse of information and the sale of non-existent products are probably the threats most related to electronic commerce, but apart from these there are many other security risks. From the above discussion it is clear that these security risks affect the Web servers, the local area networks that host Web sites, and even innocent users of Web browsers. The threats and security risks identified are categorised under the following eight categories:

1. Passive wiretapping

The passive wiretapping threat could violate customers' transaction *integrity*, i.e. changing their recorded and billed orders. Preventative measures for passive wiretapping include authentication and encryption. Eavesdropping and browser-side risks fall under passive wiretapping threats and are a great threat to *secrecy*. They include theft of information from source and destination, theft of information about the network configuration and theft about which source talks to which destination.

The **browser-side risks** include:

a) Active content (found in a web page – using for example, JavaScript) that crashes the browser, damages the user's system and breaches the user's privacy.
b) The misuse of personal information knowingly or unknowingly provided by the end-user.

An **eavesdropper** is a person or device who can intercept any network data sent from browser to server or vice versa. During this interception Internet transmissions can be copied. Traffic analysis of message movements between sites and the data sizes may reveal sensitive information. Eavesdroppers can operate from any point on the pathway between browser and server including:

- The network on the browser's side of the connection
- The network on the server's side of the connection
- The end-user's Internet service provider (ISP)
- The server's ISP

Eavesdropping leads to the *loss of information* and *loss of privacy*, which could compromise the trust of a relationship between two trading parties in an e-commerce transaction.

2. Cyber Terrorism

The FBI[2] defines terrorism as the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

Cyber-terrorism can thus be defined as the use of information technology, by terrorist groups and agents to attack sabotage-prone targets, such as, information systems and resources. Any other activities should be defined as cyber crime. Cyber terrorists normally operate with a specific political or ideological agenda to support their actions.

[2] For the definition of terrorism see URL: http://www.terrorism.com/index.shtml.

An example would be penetrating an air traffic control system and causing two planes to collide or hacking into a hospital computer system and changing someone's medicine prescription to a lethal dosage as an act of revenge.

Later in the paper it will become clear that the boundaries between some of the definitions, for example, hacktivism and cyber terrorism are so narrow. For example, some may consider an e-mail bomb as hacktivism while other consider it as cyber terrorism by others.

3. Errors and Omissions

Although errors and omissions are normally "only" *inadvertent human errors* they still are an important threat to data and system integrity. All types of users cause these errors, such as, data entry clerks, users, system operators and programmers, who create and edit data. Sometimes the errors are the threat, such as, data entry errors or programming errors. In other cases, the errors create vulnerabilities.

Programming and development errors, often called bugs, can be very catastrophic. Many programs, especially those designed by a user for personal computers, lack quality control measures. Installation and maintenance errors also cause security problems.

4. Human Threats

Human threats are due to individuals or groups of individuals that attempt to penetrate systems through computer networks or other sources. These attacks normally target known security vulnerabilities of systems. Hackers and insider attacks, although hackers are sometimes insiders, are the main components of the human threats.

Hackers are people who deliberately gain *unauthorised access* to computer systems, for whatever reason, and have a great impact on the *privacy*, *integrity* and/or *availability* of data.

The methods used by hackers to "break" into systems include [7]:

- Network spoofing
- Exploiting known security weaknesses
- Password cracking

The term "hacker" was originally used in computing circles to refer to individuals who had a low-level familiarity with the operation of technology and were capable of devising technically elegant software solutions [29]. However, the usage of the term has changed over the years. The motivation behind a hackers action may be numerous, some hackers only browse, some steal, some damage, but the fact is they are a real threat of disruption and damage to most organisational computer systems linked by networks.

Apart from external threats, a lot of attacks come from **insiders**: employees and recent past employees. Insiders (i.e. authorised users of a system) are responsible for the majority of fraud. They have both access to and familiarity with the victim computer system. An organisation's former employees, with their knowledge of that organisation's operations, may also pose threats. Therefore, it is of uttermost importance that their access is terminated promptly after their resignation. Common examples of computer-related employee sabotage include:

- Destroying hardware or facilities
- Entering data incorrectly
- Changing and/or deleting data
- "Crashing systems"
- Planting logic bombs that destroy programs or data

Computer controls and security policies will assist in protection against corporate insiders. To enforce these an access control system is needed.

5. Information warfare

Information warfare is a large field, grouping together several concepts, such as, electronic warfare, psychological warfare, information and hacker warfare. Dr. Ivan

Goldberg, a psychiatrist and clinical psychopharmacologist, describes the term information warfare as follows [138, page 1]: "The offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries." Therefore, the term "information warfare" can be used to describe the ways in which terrorist organisations could use technology to attack the IT infrastructure of a country or a particular company [32]. *E-mail spam* can be used to send false information about a company to thousands of Internet users simultaneously. This would of course affect the sales for that company of whom such misleading information has been distributed.

Denial-of-service (DoS) and direct attacks are forms of information warfare and are simply annoying and disruptive. During a **denial-of-service attack**, sometimes also referred to as necessity threat, computer or network resources are intentionally blocked, which makes them unavailable for legitimate usage and from normal processing. Of course this leads to slower processing and is normally not acceptable for users. The most common example of a denial-of-service attack is e-mail bombs. A **direct attack** takes the form of rewriting and/or stealing information, or within a computer system causing data theft. To prevent these threats firewalls could be installed.

6. Malicious Code

Malicious code, *intentionally induced flaws*, includes viruses, worms, Trojan horses and logic bombs. These techniques can result in computer downtime or data loss. The most recent high-publicity security incidents have been virus infections, data fraud and theft, and web vandalism [82].

A **virus**, such as, the Melissa virus,[3] is a special type of program (i.e. malicious program) that spreads through programs, data files, computers, or any medium, by *replicating* itself. Therefore, a virus may produce *undesirable outcomes* by "infecting" other software or programs by attaching or incorporating copies of itself into them. A computer virus is not directed at a specific user or system but always needs a host program as a carrier and must be *activated* by an external action in order to be *executed* (and cause harm). Many permutations of viruses have been created. They can infect the boot portion of any storage device, infect executable files, slowly destruct files over time and infect any type of file that has a macro attached. The most frequently encountered type of virus is the Macro virus, which is embedded into a document and activated when the recipient opens the document. They are very popular due to the fact that the language used to write macros is easy to use and the documents containing macros can be easily distributed by e-mail. User-defined macros replace system command macros, menu items, toolbar buttons and shortcut keys, and are activated by the click of a button. Physical security breaches or espionage may reveal codes to intruders.

A **hoax virus** is a false alarm spread among users about supposed viruses in order to cause scares and costs. Most virus infections are caused through floppy disks, CDs, e-mail and the WWW, containing virus-infected sites. To protect these entry points from viruses, Hruska [42, p.15] identified three main points that should deploy anti-virus software:[4] on the Internet gateway, on the servers and on the desktop (client-side).

A **computer worm** is a *self-contained program* (i.e. does not require a host program) that makes copies of itself through the network, using e-mail or some other transport mechanism and causes execution of the new copy – *without any user intervention.*

---

[3] The Melissa virus is a Microsoft Word macro virus that replicates itself through e-mail. The virus only affected people who used MS Outlook as an e-mail reader, and who don't select "Disable macros" when MS Word starts. Once any recipient activated the Melissa-infected attachment, the macro took control of Outlook and simply mailed to up to 50 people in the Outlook address book. Those recipients would also then activate the attachment and the process could continue.

[4] For anti-software procedures refer to [42].

A worm becomes a security problem when it spreads against the wishes of the system owners, and disrupts the network by overloading it. Two important characteristics related to worms are:

- They exploit flaws in the operating system.
- The release of a worm usually results in brief, but spectacular outbreaks, shutting down entire networks. Although worms are rarer than viruses they are difficult to stop once they have started spreading.

A well-known worm is the Internet worm of 1998. Good system security and closing security holes are a solution to the worm attack. Other tools used to protect a system against worms include: identification and authentication control, configuration review tools, intrusion detection tools and the firewall system.

The **Trojan horse** is a piece of malicious code that *does not replicate* or copies itself, like in the case of a virus and worm. It performs an useful function, but at the same time something more than what the user was expecting and those hidden aspects cause malicious damage. Trojan horses are threat to both the *integrity* and *confidentiality* of the system.

A computer program, which has been infected by a virus, has been converted into a Trojan horse. Viruses and "Trojan Horses" can damage encryption programs or insert procedures to allow substitute keys. Traditionally, the virus has been an internal threat, while the worm has been a threat from an external source.

The **logic bomb** is another class of malicious code that takes place when a specified condition occurs. It is in the form of a document containing macros designed to cause harm. Upon opening the document, the macrocode will run with the access rights of the target user. A variation of the logic bomb is the time bomb, whose trigger is a time or date. Word has, for example, a simple macro job scheduler, which allows macros to be set to run at some pre-defined time.

7. Web vandalism

During Web vandalism (also referred to as cyber vandalism), unauthorised persons, who are able to access a company's Web server, will upload their own web page design causing a great deal of damage [92], or do anything what an authorised person would be able to do.

8. Intellectual property threats

Intellectual property is one of the areas, which has been greatly affected by the Internet. It is difficult to protect intellectual property or to enforce copyrights, as it is very easy to copy anything found on the Internet. To trace who has obtained illegal ownership of intellectual property is sometimes impossible. In order to increase the protection (to provide some protection) of digital copyright holders the Web site access can be controlled by a password, the identity of the Web site accessor can be verified and contractual clauses can be included on a Web site. Furthermore, Internet service providers could block access to a site through packet filtering, proxy servers, or host name blocking.

To conclude, all the above threats can be classified into four main *vulnerabilities*:

- Interruption, which compromises the availability of an asset.
- Interception threatens the confidentiality of information.
- Modification and fabrication, which threaten the integrity of information.

These threats have a great impact on the *principles of information security* (which will be discussed under 4.5) and result in significant financial and information losses. They vary from data integrity threats to system availability threats and violate the privacy and secrecy of a company or even an individual.

4.4 Techniques established to ensure Security

In e-commerce security mechanisms are needed to meet security demands, such as, confidentiality, authentication and integrity (see section 4.5). Many different techniques

or security services are being used to ensure that transactions and customers are secure and/or to protect a company from unauthorised access. These techniques vary in their application. Some are best for ensuring secure communication channels while others are best for protecting servers [92]. The techniques are:

- Firewalls (protecting servers)
- Virtual private networks (protecting servers)
- Cryptography (protecting communication channels)
- Symmetric and asymmetric encryption (protecting communication channels)
- Digital signatures (protecting communication channels)
- Digital certificates (protecting client computers)
- Sniffers (protecting mainly communication channels)
- User-name and passwords (protecting both servers and clients)
- Access control list (protecting both servers and clients)

4.4.1 Firewalls

Firewalls are an important network server security measure and are the first line of defence for a corporate network [103]. A firewall is neither a product nor a service, but a strategic defensive element of an organisation's security policy. In essence, a firewall is a set of related programs at a network gateway server that help to guard company information from outside invasion and transaction validation, by allowing or disallowing the flow of incoming or outgoing information into the corporate network [105]. Therefore, the firewall acts as a *buffer between the internal network and the external world*, by controlling all the access to and from the Internet and at the same time preventing unauthorised logins to networks inside the firewall from external networks. If a company however, would divide its internal network into subsections, then an internal firewall is used it protect one area of the corporate network from other areas. In this case two internal networks belonging to one company are protected from each other. The way the network is configured depends on the security policy. For example, all FTP and Telnet requests can be disallowed, or only e-mail may go in and out the computer, or finally only incoming data is restricted.

As already mentioned, the firewall can be used to create an internal site, one that is accessible only to computers within the own local area network. The server is then placed INSIDE the firewall:

Other hosts
\
Server <-----> FIREWALL <------> OUTSIDE
/
Other hosts

To make the server available to the rest of the world it must be placed OUTSIDE the firewall.

Other hosts
\
Other hosts <----> FIREWALL <---> server <----> OUTSIDE
/
Other hosts

When the server is being broken into, the security of the inner network is not at risk, because of the firewall. Therefore, no additional software, other than firewall-specific protection software should be installed on the firewall computer. The more software installed the higher the risk of software security breaches.

Firewalls are classified into the following categories:

- Proxy servers
- Packet-level filter firewalls
- Gateway servers

Firewalls have some disadvantages. Although they provide authorisation controls, they cannot assure authentication or privacy and cannot prevent insider intrusion. Instead they assume that "the bad guys" are on the outside, which is often a very bad assumption as insiders carry out most of the really damaging incidents of computer crime. Furthermore,

firewalls are not receptive to the transfer of viruses or other corrupted files and they do not protect against message eavesdropping over the public networks, such as, the Internet. Since the eavesdropping attacks can take place outside the corporate network, the best protection for transmitted messages over the Internet is encryption. This gave rise to the idea of the **virtual private network** (VPN).

The VPN allows remote users to connect to an enterprise network and at the same time protects the data during transit against disclosure by using encryption [120]. VPN therefore, privatises the data between two network points, protecting it from disclosure and modification. This privatisation allows the transmission of data along the public network as though they were private. This does not mean that firewalls are now outdated, but a combination of both firewalls and VPNs offer new strengths needed for network attacks. VPNs will authenticate and encrypt all communications across an untrusted network, whereas the firewall will block unwanted traffic into and out of a network.

Finally, it is important to note that firewalls are only an important component of security but not a complete solution of security.

4.4.2 Cryptography

Cryptography is the *science of using mathematics* to encrypt and decrypt data or messages so that only the sender and the intended receiver can read them. Cryptography has two main tasks: providing secrecy and authenticity.

Cryptographic systems are analogised to a lock and key system, in which one party uses the key to lock (encrypt) the message, and the other party uses another copy of the key to unlock (decrypt) the message. This could be, for example, the substitution of each letter of the alphabet by another letter, dependent upon a key. These keys are measured in

lengths, expressed in bits. Keys of longer lengths are less vulnerable to a "brute force attack"[5] than keys of shorter length [1].

Cryptographic systems can be classified into one of two broad categories:

- Symmetric cryptosystems
- Asymmetric cryptosystems

In a **symmetric cryptosystem**, also called conventional cryptosystem, the same key (called the secret key) is used for both encryption and decryption. Since the keys are the same, two users wishing to communicate in confidence must agree and maintain a key. Each entity must trust the other not to divulge the key. Examples of commonly used symmetric-key systems are Data Encryption Standard (DES), Triple-DES, International Data Encryption Standard (IDEA), Fast Encryption Algorithm (FEAL) and RC5.

While symmetric cryptosystems are fast and efficient they have one challenge. The secret key from the sender to the recipient must be disseminated securely and in a tamperproof fashion over the communication channel. Surely, if one can transmit the secret key securely, one wouldn't need the symmetric cryptosystem in the first place, because the same secure channel can then be used in the first place to send the message. Transmitting a key introduces the possibility of discovering the secret key. Furthermore, to transmit a key securely, can be quite expensive. A more reliable solution is the asymmetric cryptosystem.

The **asymmetric cryptosystem**, also known as public key (PK) cryptosystem, resolves the secret key distribution issue and uses two separate, but mathematically related keys known as a key pair, which allows parties to communicate securely without sharing secret keys. No secret key is ever transmitted or shared over the open network. One key is called the private key and is kept secret by its holder and shared with no one. The other key is called the public key and is made publicly available online. If either key is used to

[5] A brute force attack is trying to guess every possible key (decryption key) that might be in use.

encrypt data, the other key is used to decrypt it to its original format. El Gamal algorithm, Rivest-Shamir-Adelman (RSA), Diffie-Hellman, Digital Signature Algorithm (DSA) are examples of public-key cryptosystems.

The public key cryptography is more suitable for a typical e-commerce transaction than symmetric cryptography, providing authentication, integrity, confidentiality and non-repudiation. It is a fundamental component of digital signatures and does not require the revealing of the private key to the communicating parties. Therefore, e-commerce firms do not need to share their private keys to anonymous online users on the Internet for e-commerce transactions.

The best approach would be to combine the symmetric and asymmetric encryption systems. SET – which will be discussed in chapter six – makes use of both encryption systems. The symmetric key, exchanged between the browser and the server, is encrypted using the public key [48].

No matter what type of cryptographic algorithm is chosen, cryptographic keys are involved and these need to be managed. Key generation, key distribution and key storage are the three main activities for successful key management. Keys should always be generated in an unpredictable way, using random bit sequences. Furthermore, when keys are generated, care should be taken that one key does not reflect any knowledge about the other key. Key distribution refers to ensuring that the keys generated are distributed between users in a secure fashion. According to Dawson [23, p. 320], there are two protocols that can assist in key distribution: key transport protocols and key agreement protocols (excluded from further discussion). Owners of cryptographic keys should store them in a secure workstation or secure storage device. Smart cards seem to offer a reasonable secure storage device and are used quite often. This means the smart cards store the cryptographic key and at the same time also perform the cryptographic work, as all the data to be encrypted and decrypted is submitted to the smart card.

4.4.3 Encryption

Encryption is a security service for a communications channel, providing *confidentiality, integrity* and *availability* of data, and is used to send sensitive information over the network from a source node to destination node. Thus, encryption is at the heart of methods for ensuring all three goals of computer security.

Encryption is the transformation of human readable text or *plaintext* (M) into a form unreadable by anyone (also called *ciphertext*) without a secret decryption key, through the application of a mathematical computer algorithm. Using *decryption*, the ciphertext is reverted to the original plaintext. An attacker may either try to obtain the secret key or to recover the plaintext without using the secret key. In a secure cryptosystem, the plaintext cannot be recovered from the ciphertext except by using the decryption key.

The security of the encrypted data is entirely dependent on the strength of the secrecy of the *unique key*.[6] However, the strength of the encryption system is dependent on the algorithm [48]. The key size is measured in bits and the bigger the key; the more secure the ciphertext. The current Data Encryption Standard (DES) cracking project is able to break the encryption for a 56 bit DES in twenty-two hours [46]. As long as the key remains secret, the system also provides authentication.

Encryption can be subdivided into **three functions** [92]:

- Symmetric encryption or private key encryption
- Asymmetric encryption or public key encryption
- Hash coding

Figure 4-1 and Figure 4-2 illustrate the symmetric and asymmetric cryptosystems. Using the ***symmetric encryption*** system, the same key (K) is used to encode and decode data. Both parties share a secret key, allowing them both to encrypt information in order to

[6] A value that works with a cryptographic algorithm to produce a specific ciphertext.

send it to the other party as well as decrypting information received from the other party. The symmetry of this situation is a major advantage. With the ***asymmetric encryption*** system, keys come in pairs: one key is used for encoding and another for decoding. The decryption key K_d, inverts the encryption of the key K_e. For example, let Alice's public and private keys denote as AK_e and AK_d, and Bob's public and private keys as BK_e and BK_d respectively. In the latter case, if Alice wants to send confidential data to Bob, she needs to encrypt it with Bob's public key $BK_e(M)$. Bob, and only Bob, will then be able to decrypt it with his corresponding private or secret key $BK_d(M)$.

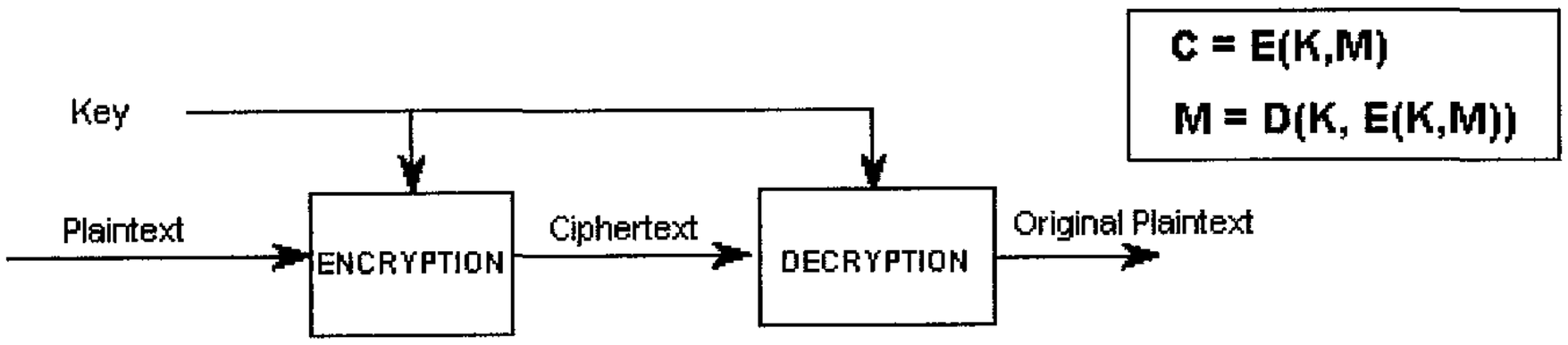


Figure 4-1 Private Key (Symmetric) Cryptosystem

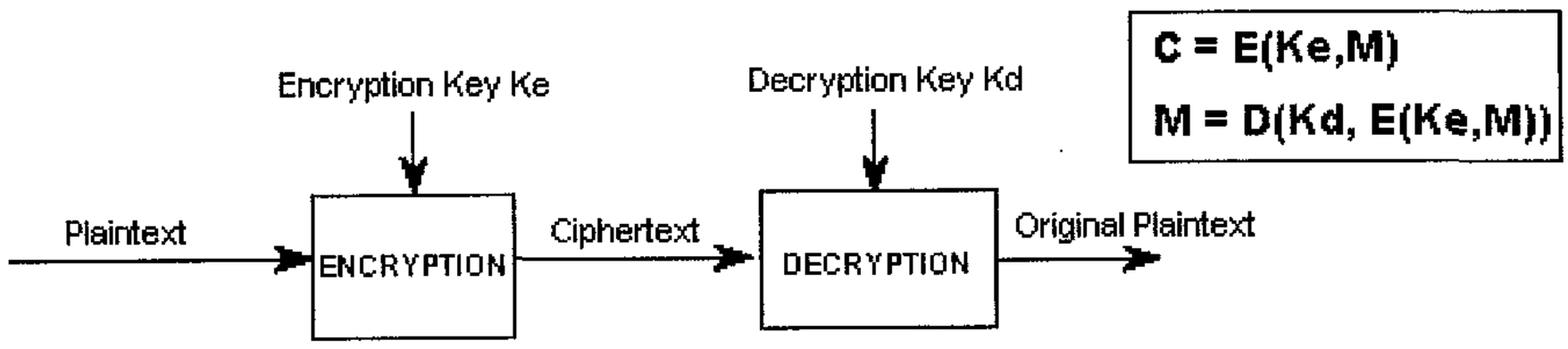


Figure 4-2 Public Key (Asymmetric) Cryptosystem

Public key encryption can be used as a method to achieve *confidentiality* and for employing *digital signatures*. As just mentioned in the previous example, anyone who needs to send a message can encrypt the message with that person's public key such that $C = EK_e(M)$. Only the person who has the corresponding private key can decrypt the information, making it safe from interception and at the same time achieving confidentiality. But this message provides no assurance to the recipient that the message truly came from the sender. In order to achieve this assurance a digital signature can be created using the private key to encipher the message and the public key to decipher the message. In this case $M = DK_e(EK_d(M))$. Combining these two scenarios, authentication of the sender and message confidentiality can be provided at the same time. The sender

first encodes the message with his own private key and then encodes it again with the recipient's public key. Upon receipt, the recipient first decrypts the message with his private key and then decrypts it with the sender's public key.

Compared to symmetric encryption, public key cryptography has a lack of performance, i.e. is slow (at least 100 times slower in software and 1000 times slower in hardware) and produces enormous volume of data. The ***one-way hash function***, also called message digest function, is an improvement on this scheme and ensures that a message is not altered during transmission, in situations where encryption is not used. The one-way hash function does not use a key, but takes a message of variable-length input to calculate a hash value (fixed-length number) using a hash algorithm [92]. The hash value is a signature for the message. The message and message digest are encrypted with the senders private authentication key and delivered to the receiver. If the received message does not generate the same hash value from the source message, but an entirely different output, the receiver knows that the original message was changed or tampered in some way. Hashing functions in use today are SHA (Secure Hash Algorithm) and MD5 (see below).

Various **algorithms** and **standards** have been developed to encode information, among them being:

- DES, a popular symmetric encryption program that has been accepted as a cryptographic standard in the United States and abroad.
- MD4 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "message digest" of the input. The MD4 algorithm is intended for digital signature applications.
- MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "message digest" of the input. Ron Rivest designed MD5 to fix a weakness, which was discovered in MD4. The MD5 algorithm is therefore, an extension of the MD4 message-digest algorithm and includes optimisations and suggestions made by reviewers.

- SHA is a standard hash algorithm, designed by the U.S. National Security Agency (NSA).
- RSA is a public-key algorithm used for both authentication and encryption.

To ensure secure traffic and communication over the network, **standards** and **protocols** have been developed:

- Secure Sockets Layer (SSL) Protocol
- Secure HyperText Transfer Protocol (S-HTTP)
- Pretty Good Privacy (PGP)
- Secure Multipurpose Internet Mail Extension (SMIME)

Both SSL and S-HTTP are proposed encryption and user authentication standards for the Web. Each of them requires the right combination of compatible browser and server to operate.

4.4.3.1 Secure Sockets Layer (SSL) Protocol

SSL ensures secure transfer of information over the web. All the data flowing between the client and the server is encrypted and then decrypted. SSL was originally developed by Netscape and has been adopted, as protocol, to encrypt transactions in *higher-level protocols,* such as, HTTP, NNTP and FTP. Meaning, SSL is a protocol on top of the transport like, TCP/IP, HTTP, Telnet, FTP and NNTP [95], to enable encrypted communications across the Internet. SSL is not an electronic payment system, but a transmission protocol used to provide security [136]. This protocol is mostly used for server to client communications.

The primary use of SSL was to enable secure credit card transactions across the WWW, by using a private key to encrypt data (i.e. credit card numbers) that's transferred over the SSL connection and providing authentication of the merchant. The important *security principles* provided by SSL are [65]:

- Privacy and confidentiality

- Client and server authentication
- Message integrity

SSL makes use of *public-key encryption* and *private-key encryption*. As already mentioned, private-key encryption is faster, while public-key encryption provides better authentication. Therefore, public key cryptography is mainly used only for digital signatures and message authentication.

When SSL is used to secure payment the merchant operates on an SSL-enabled WWW server. If the client requests for a web site address (URL) that starts with "https://" instead of "http://" he knows that the data transfer is secure. Therefore, the server will first authenticate itself, after which the buyer can send his credit card details to the server [79]. The SSL connection comes in two strengths: 40-bit and 128-bit [92].

How is a SSL connection (handshake) established?

In an SSL connection each side of the connection must have a security certificate, which each side's software sends to each other. A browser (or client) can ask the server to confirm his identity by asking for a digital certificate. This is especially useful when the user sends sensitive information, such as, the credit card number, to the server.

The server sends his certificate and public key, issued by certification authorities (CA's), to the user and may ask for the client's certificate. The client can then extract the public key from the server's certificate to verify its authenticity. An encrypted and authenticated connection cannot be established, if the server cannot be authenticated. The client sends his encrypted private session key (using the server's public key) and certificate to the server. The server decrypts the message, using his private key and generates the shared private key, also known as the session key. The session key is then used to encrypt and decrypt all the messages and to verify data integrity.

4.4.3.2 Secure HyperText Transfer Protocol (S-HTTP)

S-HTTP operates at the application layer and works only with the HTTP protocol. In fact, S-HTTP is an extension to HTTP that provides client and server authentication, spontaneous encryption and non-repudiation [92]. Both public-key encryption and symmetric encryption are provided by S-HTTP. The difference between SSL and S-HTTP is that SSL makes use of a handshake to set up a secure communication, whereas S-HTTP makes use of packet headers to set up a secure connection. Messages are then send using an envelope.

4.4.3.3 Secure Multipurpose Internet Mail Extension (SMIME)

SMIME (or also seen as S/MIME) was designed to solve the problem of interception and forgery of e-mail. It is a specification for secure electronic mail and was designed to add security to e-mail messages in MIME format and to be interoperable, so that any two packages that implement SMIME can communicate securely. The security services offered, are authentication (using digital signatures) and privacy (using encryption).

S/MIME is not specific to the Internet and can be used in any electronic mail environment. S/MIME attaches the digital signature first, and then encloses the signature and the original message in an encrypted digital envelope. In this way no signature information can be exposed to the eavesdropper. The digital certificate used, is the X.509 format.

Compared to PGP some differences can be found. PGP relies on users to exchange keys and establish trust in each other. This works well for small workgroups, but can become unmanageable for large numbers of users. S/MIME, on the other hand, utilises hierarchies in which the roles of the user and the certifier are formalised. This means that S/MIME is both more secure and more scalable than PGP implementations [153].

4.4.3.4 Pretty Good Privacy (PGP)

PGP [151] is probably the most widely used application for securing electronic mail. Under the conventional cryptosystems, secret keys need to be exchanged, which is a big drawback in the area of security. PGP solves this problem. Instead of having only one key that two parties have to share, every user has two keys, a public one and a private one. If the public key encrypts a message, the message can only be decrypted again with the private key, and the other way round. Therefore, PGP brought encryption technology to the average desktop computer user.

4.4.4 Digital Signature

A digital signature is the same as a hand-written signature, except that a hand-written signature can easily be changed, whereas a digital signature can nearly never be changed. A digital signature creates a **unique electronic signature** for an individual, which can bind the sender to the text of his message, i.e. bind information to an entity, avoiding denial by the sender that he or she never sent the information. Such a signature enables the recipient of the information to verify the authenticity of the information's origin, and to check that the information has not been altered, achieving a great deal of trust. Therefore, the security features provided by digital signatures include: *authentication, data integrity* and *non-repudiation* (see section 4.5 for definition of concepts).

Blind signatures have applications when the sender does not want the signer to be able to observe the document content or sender identity.

Current digital signature technology makes use of several types of asymmetric cryptography based on algorithms. DSA is one of these algorithms. DSA uses a hash function to produce a message digest. The digest is then processed with the private key plus a random number, to generate two 160-bit numbers as a signature. The recipient uses the digest, the originator's public key and on half of the signature pair to produce the other half of the signature pair [65]. If both values are the same, the signature is verified.

In short, a digital signature can be used to establish trust between parties in an electronic transaction when traditional forms cannot easily be used. It is used to provide proof of origin, proof of delivery, proof of submission and proof of electronic transport [29].

4.4.5 Digital Certificates

Under public key cryptography, one key part of the key pair, corresponding to a specific individual, is published on the network, for other users to retrieve. After retrieving, how do these users know that the public key is authentic, i.e. belongs to the individual who published it or that the message was indeed sent by the person who claimed to send it? This is where digital certificates are useful, *associating a public key with an identity*. Certification is the endorsement of information by a trusted entity, whereas a digital certificate constitutes the digital identification of a user or device [1]. It is a document, containing the public key of an entity, the identity of the owning entity, and some other identification, all of which is then signed with the private key of the certification authority (CA), guaranteeing that the public key actually belongs to the named user.

Digital signatures use the digital certificates to ensure an even greater level of security. The digital certificate plays a big role in authentication as it legally binds the digital signature to its owner, i.e. assures that a participant is ***authenticated***, and can be used within a web page or an e-mail message. In the same way as a user can request the server to send a certificate, the server can request the user to send a certificate.

4.4.5.1 An Universal Certificate Format

All the application systems participating in electronic payments will be of wide diversity. A standard is needed to represent cryptographic information before it is sent across the network [79]. **X.509** is the standard for digital certificates and the internationally recognised specification, supporting security frameworks as they apply to electronic commerce. The authentication framework, as spelled out in X.509, addresses the

handling of public keys using certificates. Any application system or device can use a X.509 certificate to link identities with the corresponding public key.

4.4.5.2 Certification Authorities (CA's)

A certification authority (CA) is a *trusted third party* that verifies identification, creates a recognised and trusted document that *certifies identity* and issues the document. To ease their tasks the CA's could use the public key infrastructure (PKI) technology.

An entity requests a certificate from a certification authority when he needs to obtain proof of ownership for a public-private key pair that he will use during an electronic transaction. The entity will generate a public-private key pair, of which the public key is sent to the certification authority. If the request satisfies the CA's certificate issuance policy [31], the CA will issue a certificate to the requesting entity. Therefore, the authority binds the identity of the certificate owner to the public key contained within it.

For any transaction the entity sends the transaction details along with the certificate to the buyer. The buyer will use the certificate to determine whether the seller is who he claims to be. In the same way a seller could use a certificate to determine whether the buyer is who he claims to be.

A certificate is only issued after the CA checked the background of the business or individual. Certification authorities do however, not only create and assign certificates for verifying digital signatures (i.e. certification management), but also revoke and recover[7] them under certain circumstances.

CA's control among other things the firm's certification policies, practices and underlying cryptographic algorithms. With the increased use of digital signatures and

[7] Certificate revocation makes a certificate ineffective permanently for a specified time forward. Certificate recovery enables keys, if lost, to be reinstated.

certificates, two types of CA solutions have emerged:

- Enterprise CA's
- Commercial CA's

Enterprise CA's are controlled by the firm itself meaning the firm is the root CA in an enterprise solution. The firm writes its certification policy and practice statements, installs the CA, establishes roles and attributes for the use of digital signatures, maintains the algorithms etc.

Commercial or **retail CA's** retain all the functions of the root CA. Certification policies and practices statements are written by the retail CA's and not by the firm itself. VeriSign, [8] one of the best-known CA e-commerce providers has built its entire business on retail digital signatures and certificates.

4.4.6 Sniffers

Sniffing can be viewed as a threat but also as a security technology. Sniffers are *programs* designed to tap or intercept into the Internet and capture certain information [95]. This can be very useful for administrators and trouble-shooters who want to analyse the network's activity for example, and pinpoint where a problem is occurring. Unfortunately, as soon as this software is used unauthorised, it becomes a risk to businesses. Hackers, for example, may use them to spy on the network and steal unauthorised information like passwords. Once the perpetrator has the connection to the Internet and the sniffer software he just needs to wait for sensitive data to pass through the communication channel [36].

[8] VeriSign's homepage is found at URL: http://verisign.com/

4.4.7 Passwords and Access Control (AC)

One of the key elements in controlling access to certain information on the web or to a computerised information system is identification of the user to whom access is to be granted. Every user should therefore, be able to identify himself and to validate his identify before being granted the necessary access. This *identification* and *authentication scheme* normally consists of a username and a password transmitted over the Internet. Passwords have on purpose: to uniquely identify an individual as having some type of authorisation [105]. Subsequently, users who do not enter the correct password will not be able to use or even log into the system. People should very carefully select their passwords, avoid sharing them with others and never write them down. The following points should be considered when creating passwords:

- Try to use a combination of upper and lower case and non-alphabetic characters.
- Do not use a word in any language. Hackers can use dictionaries to track the password.
- Try to avoid obvious patterns. For example, 666666 or 123456.
- Avoid geographical names e.g. Australia.
- A password should be changed from time to time.

Biometrics is another authentication technology and assures the highest accuracy. The physiological (such as, fingerprints) and behavioural characteristics (such as, voice) of a human are being used for identification.

The access, read and write privileges of every user, or class or users to system resources may be limited through access control (access rights) or access authorisation. Access control should however not be confused with authorisation. Access control guards against improper entering, usage, interaction and access of a network, a zone, a service or a transaction. Whereas, authorisation grants access to functions or services within a given zone of access [48]. Determining access control for all resources involved in an electronic transaction will enforce electronic controls and reduce the risk of unauthorised access. Access control can be handled using the *access matrix*. For each subject a list of

accessible objects are specified, and for each object a list of subjects who are permitted access rights.

4.5 Principles of Secure Computing

A number of "security services" must be delivered by a system of electronic communications if it is to be considered secure or trustworthy. These services, which form the basic elements of information security, are data confidentiality, identification and authentication, availability, integrity, and non-repudiation. The application of these services will build the TRUST in e-commerce, which users require.

Confidentiality, implying exclusive knowledge, refers to the assurance that the information sent from a sender to a receiver is available only to the intended receiver, i.e. authorised party and not disclosed to unauthorised individuals [95]. In electronic commerce, keeping order details and credit card information confidential during transmission is a major security concern [102]. Data confidentiality can be achieved through the use of *encryption*. Confidentiality is sometimes called *secrecy* and *privacy*, which are closely related. According to Schneider and Perry secrecy refers to "protecting against data disclosure and ensuring the authenticity of the data's source" [92]. Privacy, on the other hand, means "the right of the individual or entity to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed".[9] Therefore, the individual right of a person is protected.

When using the web, information about the particular web browser can be retrieved. Information, such as, from which site you are coming, which browser you are using and your Internet address. Use of this information by an unauthorised user can breach secrecy and privacy on the Internet.

[9] RFC 2828: Internet Security Glossary; May 2000.

Privacy in e-commerce is compromised in two ways: by the use of cookies and the involvement of law enforcement agencies. Cookies are small text files written to the client's hard drive by some Web sites that are viewed by the client's browser. They were developed to personalise information, help with online sales or services, and for the purpose of tracking popular links or demographics. Although cookies are a useful tool for web site developers, they upset a lot of users at the same time as they rise concern about security and privacy. They are enabling developers to get a sense of whom they are dealing with and what path the user is taking through the site. The problem with cookies is, if they stay on the client' PC. Marketers can build up a history of user preferences, based on the web sites accessed by the client. This is invasion of privacy. Furthermore, the cookie file is a text file that is easily read. If an unencrypted password is placed in this file, the danger of this file being read by some other malicious mechanism is a potential exposure.

An **identification** security service provides a means of identifying communication parties. The verification of these communication parties is provided during authentication. **Authenticity** is the process of confirming user identity or data origin and integrity. This refers to the need for the receiver to be assured that the data truly came from the alleged sender. Electronic authentication is achieved through the use of public key cryptography, shared secrets (such as, passwords and PINs), biometric devices and digital signatures. These technologies can be combined to provide even stronger levels of authentication or security. Alice could encrypt confidential data with her private key, known only to herself, and enclose that in the digital envelope. Bob, or in actual fact anybody who holds Alice's public key, would or could decrypt the message with Alice's public key – proving that Alice sent the message, as she is the only person who holds the private key (provided the key is not stolen) [68]. To ensure Alice was the person encrypting the message, her identity must also be proven, as anybody who holds her private key could encrypt the message. Certification authorities provide this identification. According to Pohlmann [84, page 12] things needing identification (tell me who you are) and authentication (prove to me who you are) are communication partners,

communication media, messages, authorisations and access controls. Electronic cash is one parameter, which is better off unauthenticated.

Availability, also known by its opposite, denial of service, means that the hardware, software and data should be accessible only to authorised parties. During a denial-of-service attack, network and computer resources are intentionally shutdown, blocked or degraded, making them unavailable for legitimate usage. The goal of such attacks is to flood the communication ports and memory buffers of the target site. For businesses on the Internet lost time means lost sales and lost revenue. E-mail bombs are one method of this type of attack. Tamil Tigers against Sri Lankan embassies around the world carried out the first recorded cyber terrorist denial-of-service attack [32].

Unauthorised data changes (e.g., adding, deleting a message) results in the violation of integrity, which occurs whenever a message is altered while in transit between the sender and the receiver. **Integrity** is concerned with ensuring that data from a sender to a receiver has not been subject to unauthorised modification or destruction during its transit. Therefore, integrity implies certainty. For electronic commerce, integrity ensures that information, such as, order details or payment information has not been modified [48]. For example, the change of a book order can have a big effect on the consumer's credit card. Instead of only ordering one book, it can be changed to 10 copies. Integrity can be provided through a *one-way hash algorithm*. Alice could use the hash algorithm on the message before encrypting it with her private key. The message is added to the digital envelope. On receipt, Bob can decrypt the message digest with Alice's public key, and generate a new hash value from the received message, using the same hash algorithm. If the two hash values (received and calculated) are the same the integrity is verified, meaning, the message received is the same as that sent. Using this process, the two parties can prove that their communications have been confidential, unaltered and actually took place [68].

Non-repudiation, partially ensured through integrity and authentication, prevents parties from denying a transaction's validity or it's existence [68]. For example, a seller that receives an order wants to be able to prove, if necessary, that the buyer placed an order.

Digital signatures are an important security mechanism for generating non-repudiation evidence and are used in security services, such as, authentication and non-repudiation. The security requirements[10] that need to be achieved by a digital signature, differ when used for different purposes. For authentication, the digital signature must only be valid at the time of verification. However, for non-repudiation the signature must stay valid until its expiry date [88]. For example, the public key, i.e. signing key could be forged after the signature was generated. Although the public key should be revoked when forged, the signature should still remain valid. Otherwise a signer could deliberately forge the signature key, after generating the certificate, in order for his signature to become invalid. To overcome this problem, a trusted time-stamping authority can be used to secure digital signature as non-repudiation evidence.[11]

Using cryptographic techniques, the principles of secure computing can be achieved. Digital signatures, certificates and certification authorities ensure authentication and authorisation. Hashing guarantees message integrity. Encryption provides confidentiality and privacy for the message of a file as a whole. Symmetric cryptosystems support authentication, data integrity and confidentiality, and public-key cryptosystems support all five information security principles. The best electronic commerce security uses all these variants of cryptographic technology.

4.6 Establishing Security Policies

To avoid or minimise security risks and to protect a system's integrity, privacy, and necessity and authenticate users, a written security policy should be created. A security policy consists of a set of security principles and directives (rules and regulations). It dictates the behaviour of users within an organisation and determines the company's position towards security. Without a written policy, it is difficult to implement any security at all, as the security policy will dictate the security controls needed to ensure efficient security levels.

[10] See Appendix E for an overview of the security issues and security techniques.
[11] See Article [88] for more information on time-stamping authorities.

The security policy should specify policies with regards to (of course this list does not cover everything):

- What computer resources and/or network resources must be protected?
- Why the computer resources and/or network resources are being protected?
- Which resources are available to protect the assets that have been identified?
- User-level security policies, i.e. who should have access to the network and/or computer system and who not?
- When users are allowed to access the network system and/or computer system.
- What they are allowed to do (different groups may be granted different levels of access), e.g. who is allowed to view selected information and who is allowed to change data?
- Behaviours, which are acceptable and not acceptable.
- Procedures for granting access to the system.
- Procedures for revoking access (e.g. when an employee leaves).
- What constitutes good passwords for login?
- Remote and local login methods.
- System monitoring procedures.
- Protocols for responding to suspected security breaches.

A written security policy helps every staff in the organisation, whether administrator or normal user, to understand the meaning of a security policy and what is and is not permitted on the system. For example, a security policy could inform employees of their Internet security responsibilities and restrictions. Subsequently, the written security policy will raise the level of awareness in security.

Apart from the above, the security policy should cover physical security, network security, access authorisations, virus protections and disaster recovery plans. The disaster recovery plans should be reviewed regularly as the threat conditions change.

4.7 Conclusion

As more and more people will access the Internet to conduct their transactions online, security is becoming an important concern in electronic commerce. More and more crimes are being reported on the Internet, as this communication medium has not only provided an attractive business channel, but at the same time a new medium for criminals to conduct their crimes. Using the Internet, crime is easy to conduct, as the criminals do not need to be physical present (for example in order to access data files), they are not faced with physical borders and evidence is hard to collect.

The evolvement of the various criminal threats, security risks and the desire to achieve the primary security issues namely: confidentiality, identification and authorisation, authenticity, availability, integrity and non-repudiation, have created a need for the development of security techniques. Several approaches on how to implement security, control access to electronic resources, authenticate and verify individual users, protect the contents of electronic transmissions (such as, electronic transactions) and ensure integrity of data, are available today. One method of increased security is to use techniques or controls, such as, cryptography, hashing, public key infrastructure technology, digital signatures, digital certificates, passwords, tokens, biometric devices and firewalls. These existing security technologies should be built and/or enhanced in such a way in order to provide the basis for trust in e-commerce among participants and to achieve the goal of a secure e-commerce environment.

Chapter 5

Traditional Payment Systems

Everything ... must be assessed in money; for this enables men always to exchange their services, and so makes society possible.

Aristotle (384 – 322 B.C.) [79].

5.1 Introduction

Cash, cheques, debit cards and credit cards are the traditional payment system mechanisms, used to exchange value in transactions for goods, securities, and services. This chapter outlines these payment systems briefly.

5.2 Cash

Currency or cash came only into service during the first millennium B.C. in Lydia, an area now a part of Turkey [105]. Traditional payment systems have utilised cash to effect low-value, high-volume transactions. When cash, being the most simplest and effective form of payment, is used to enable a transaction, payment involves the exchange of value along with settlement. This is because the currency represents final payment. Cash offers both **privacy** and **anonymity**, as it leaves no audit trail, meaning no information is left behind in order to determine the transaction history. As of today cash is readily acceptable, being the most popular form of money transfer, and can be immediately used in another transaction. Paying for goods or services of large amounts, i.e. carrying large amounts of cash in a wallet is attractive to thieves and gives rise to some security concerns. Nevertheless, cash is the most commonly used form of payment. The

development of the automated teller machine has made cash such a dominant way of payment, allowing easy access to money [79].

5.3 Conventional Cheques

A cheque is a signed paper document that orders the signer's bank to pay an amount of money from the signer's account after a specified date. It is a convenient form of payment if users do not want to withdraw cash in order to make a payment. Cheques have the advantage that they pass directly from the payer to the payee, so that the timing and the purpose of the payment is clear to the payee.

A consumer writes and authenticates a cheque among purchase and passes it to the merchant (cheque recipient), who may endorse it with a signature before presenting it to a bank for payment. After receiving the cheque, the cheque recipient will first deposit this cheque in his own account. If the merchant's bank and the consumer's bank are the same, the bank simply transfers the funds from the consumer's account to the merchant's. If the merchant's bank and the consumer's bank keep accounts at different banks, the merchant's bank, as his collecting bank, presents the cheque for settlement to the consumer's bank (paying bank) and receives the funds accordingly. Consumers receive statements from their banks showing which cheques have been paid. Therefore, when a cheque is tendered in exchange for a good or service, a transaction takes place, but the actual exchange of value is contingent upon being able to collect the cheque from the bank the cheque is drawn upon.

Using a cheque works equally well when there is a negative balance in consumers accounts, at least if the consumers' banks are willing to extend credit--that is, to lend the consumer's funds needed to pay off the cheques. A credit card (see section 5.4 below) is another example of an account that lends money to the consumer.

One disadvantage with cheques arises when the consumer has no funds, leaving the cheque recipient in possession of a *dishonoured cheque*. This is due to the fact that when a merchant receives a cheque he does not know yet if the consumer has adequate funds until presenting the cheque to the paying bank for deposit. Therefore, cheques, as a payment mechanism, introduce uncertainty to some extent. Furthermore, paper-based cheques are very expensive to process, especially for dishonoured cheques.

By comparison with cash, when a cheque is used in a transaction, the cheque does not represent final payment and cannot be used immediately in another transaction.

5.4 Credit Cards

VISA International and MasterCard are the two major card associations, currently in place, handling settlement of credit card purchase. A credit card is an account that lends money to the consumer meaning, consumers are allowed to purchase goods or services on credit. The credit card, being a token of trust, transfers the risk of granting credit from a merchant to the card-issuing bank. Both consumers and merchants must register with a bank.

The participants involved in credit card payments include [158]:

- *Customer/Cardholder*: The consumer doing the purchase, using a credit card that has been issued by its issuer.
- *Issuer*: The financial institution (i.e. bank) that issues the card to the cardholder. The issuer guarantees payment for authorised transactions.
- *Merchant*: The merchant offers the goods and has a financial relationship with the acquirer.
- *Acquirer*: The financial institution of the merchant. The acquirer processes credit card authorisations and payments.

The biggest advantage of credit cards is the fact that they are honoured internationally. But, although credit-card-based systems have the advantage of seeming familiar to consumers, they don't do everything cash can:

- They are not anonymous
- They do not work person-to-person
- They have credit limits

5.4.1 Traditional Credit Card Purchase Process

In the case of conventional purchases, the customer or cardholder presents his or her credit card at the cash register to the merchant, who registers with a credit card company. The merchant's cash point records the name of the credit card company, the credit card number, and the validity date. This data as well as the purchase amount and the date are noted on the receipt, which is then signed by the cardholder. The cardholder receives a copy of the receipt, ensuring that the invoice total cannot be changed at a later date. In this way the *integrity* is protected. The cardholder's signature acts as authorisation for the bank to transfer the amount in question from the cardholder's account to that of the merchant. Once payment is received, the merchant can verify the signature's *authenticity* by comparing it to the signature provided on the back of the credit card. This authentication is necessary in order to ensure whether the customer has sufficient funds for the payment. The embossed number on the credit card verifies the consumer's account number. For settlement, which occurs after the purchase has been shipped, the merchant must submit the transactions to his acquiring bank, which will settle the transactions with the card issuer. The merchant's account is credited, while debiting the account of the cardholder.

Nowadays, the card data is captured through the card's magnet strip, and the purchase amount can be confirmed online. During this process, the card's validity and the balance available is checked before any purchases can be made. In this process, the card itself and the cardholder's signature identify a cardholder.

The merchant is assured of payment of a transaction, once the purchase is authorised by the card issuer over the private authorisation network. At the same time, the card issuer assumes responsibility for billing the consumer and collecting the money. However the issuer is only responsible for the risk of non-payment. The merchant bears the risk of fraudulent card usage and pays the credit card transaction costs.

5.5 Limitations of Traditional Payment Systems

Apart from the fact that the traditional payment systems are in use for some time, they do have some problems and/or limitations. Some of the issues are:

- *Non real-time payments*. As cheques and credit card payments are not in real-time there is a delay in processing the payment. This introduces a financial risk for the business. Depending on the type of payment, the realisation of a transaction may take up to a couple of weeks.
- *Lack of convenience*. To close a transaction, physical presence is needed. Both parties the merchant and the consumer must always see each other in person or communicate over the phone. Of course this is very inconvenient for the consumer and for the merchant it may mean a loss in revenue.
- *Lack of security*. Cash and cheque are particularly safe, but credit card payments are less secure. Furthermore, signatures can be forged, credit card numbers can be stolen, customers may not settle their bills, insufficient funds can exist in customers account, or merchants can commit fraud.
- *Higher cost of payments*. For smaller transactions the cost of a transaction may exceed the value of the sale item. This is also the reason why traditional payment systems are sometimes not applicable for micro-payments.

5.6 Conclusion

Electronic commerce gave rise to the need of electronic payment systems. Some of the above discussed payment mechanisms may be supplemented or surpassed by the "new" payment mechanisms for electronic transactions. However, they cannot be replaced, due to various reasons. People, who do not have access to the Internet, especially the people in the third world countries, will not be able to conduct their transactions on the Internet. Even those people, who have access to the Internet, are very sceptical about e-commerce due to the perceived security risks and threats associated with electronic transactions over the Internet. This group of people will definitely make use of the existing traditional payment mechanisms!

Chapter 6

Electronic Payment Systems

Anyone who wants the world to stay as it is,

does not want it to survive.

Erich Fried (Austrian writer, 1921-1988).

6.1 Introduction

The Internet is becoming a commercial place in which payments are rendered for goods, information and services. To support such e-commerce some form of money must be exchanged over the Internet. A *secure* payment method - electronic payment system - is required as a compensation for information, goods and services provided on the web (for example, access to copyrighted materials) and as a convenient way to pay for external goods and services. It helps to automate sales activities, extends the potential number of customers and may reduce the amount of paperwork.

Today, there exist a wide variety of electronic payment systems - most of them incompatible with each other. The broad categories of electronic payment systems are [158]:

- **Electronic cash-like and token-based systems**. In these systems, transactions are performed with tokens that have a certain value, purchased from a central authority [44].
- **Notational cheque-based systems**. Cheques are payment instruments whose validity requires reference to the issuer.
- **Notational credit systems**. Credit card payment schemes provide a payment mechanism through the existing credit card payment infrastructure. These schemes have many structural similarities to cheque models.

- Systems supporting the **secure presentation of credit card numbers**.

All electronic payment systems have different strengths and weaknesses with respect to the requirements for an Internet payment system: security, reliability, anonymity, flexibility, scalability, robustness, acceptability, cost effectiveness, ease of use and ease of integration. This chapter explores the various e-commerce payment mechanisms found under their respective categories, according to their strengths and weaknesses, specifically with respect to security. Some of these payment mechanisms are variations on traditional commerce payment methods, while others are different [36].

6.2 Security Concerns

Companies are faced with the task to track and verify (i.e. authenticate) electronic payment information in order to resolve disputes and protect against fraud and wrongful manipulation while at the same time protecting the privacy of customers. These conflicting aims are not easy to achieve when developing and/or incorporating electronic payment systems. Any payment system should consider the privacy of the consumer and the safety of the payment itself [13]. A consumer's privacy is protected when nobody else knows about his/her transaction, whereas the safety of the payment is achieved, when payment can be made without any unauthorised party intercepting.

Digital cash can be ported from one place to another, without being in physical possession of the cash. Physical possession normally implies ownership of cash and identification of an individual, which will of course no longer be the case with digital cash. The parties involved in an electronic transaction, i.e. payer and payee need to be identified thoroughly using methods, such as, passwords, cryptographic keys, electronic signatures, fingerprints and biometric identification.

At the same time, parties, using electronic payment systems, must be assured that any information exchanged will be transmitted only to the authenticated parties and payment

mechanisms, and only to the extent to which they are authorised to receive the information - in fact, ensuring anonymous financial transactions. Authorisation has traditionally been accomplished by providing the paying party with a receipt that represents an indisputable proof of payment to the intended recipient.

The payment system must control and prevent serious threats, such as, deception, fraud, embezzlement and money laundering. Useful tools to combat these threats include encryption, passwords, digital signatures, and the detection of suspect patterns.

Signatures and confidentiality are the two biggest problems in creating digital payment instruments. These issues are typically handled with some form of cryptography. The use of public-private-key pairs allows a message to be "signed" digitally and verified by anyone who has the public key. Some form of public-key infrastructure, such as, certificates, must be employed to associate a named user or an account unambiguously with a particular public key.

6.3 Electronic Wallets

The electronic wallet represents an important development in the move towards a cashless society and is used by many electronic payment systems. The electronic wallet is a device for making payments electronically rather than using cash.

According to Jupiter Communications,[1] 27% of Net shoppers abandon their offers before completion, because of the hassle of entering personal information over and over at the checkout point. Whenever a user wants to make an online sale or purchase, most online merchants ask him/her to enter their address and payment method information into a Web-based form. This procedure can be very tedious and inconvenient and this is exactly the problem that electronic wallets should resolve.

[1] Jupiter Communications homepage at URL: http://jup.com/home.jsp

6.3.1 How does an Electronic Wallet function?

An electronic wallet contains credit cards, electronic cash (for example the CyberCoin Wallet), owner identification, and owner address information. At the electronic checkout site's counter the information is provided in order to complete the checkout process and close the sale. Therefore, after customers have filled up their electronic charts, they do not need to fill in all the information requested on the forms at the checkout counter. The electronic wallet will fill-out the required information automatically. Apart from this the electronic wallet may be used to gain access to electronic cash and information services, and for identification purposes.

The World Wide Web Consortium (W3C) is trying to standardise the electronic wallets. An industrial consortium including AOL, IBM, Microsoft, Visa and MasterCard have agreed upon a common technology called Electronic Commerce Modelling Language (ECML) for electronic wallets (see section 6.3.3 Electronic Commerce Modelling Language (ECML)).

6.3.2 Advantages and Disadvantages of the Electronic Wallet

The advantages of electronic wallets are:

- Makes online shopping more efficient because consumers do not have to repeatedly enter their shipping and payment information with each transaction. The forms are completed automatically upon the user's request.
- Functions as convenient and secure Internet payment method.
- Stores purchasing data securely.
- Usable for micro-transactions.
- Supports Navigator and Internet Explorer.

The disadvantages of electronic wallets are:

- The wallet downloading process is very slow. This is however changing already, as more and more wallets are not required to be downloaded by users. One example is

PowerWallet from the Company Qpass. Transactor Networks' wallets also try to avoid the downloading process.

- An electronic wallet "lives" on the client's computer. Meaning, if one wallet is used at home and another one at work then the wallet information cannot follow the person when moving around.

6.3.3 Electronic Commerce Modelling Language (ECML)

ECML, announced in June 1999, is the *universal format for digital wallets* and merchant Websites. It is a technology, that should replace the completing electronic wallet standards with one single standard and that will allow customers to shop with one-click across a variety of Web sites.

ECML provides a set of uniform field names and content specifications plus a few procedural guidelines for the transmission of basic address and payment information from a customer-to-merchant. Therefore, ECML is a very simple way to smooth customer to merchant communication and to simplify online purchases by bringing the merchant and consumer together. Once a consumer has filled in the information, it will automatically be used to complete the purchase applications of participating sites and to subsequently close the sale.

Previously vendors did not accept ECML because they wanted to have their own standard. The ECML Version 1.0 was developed by an industrial consortium and is documented in RFC 2706.[2] ECML Version 1 is not a replacement or alternative to SSL/TLS, SET, XML, or IOTP. The goal is to develop Version 2, which may include corrections to the Version 1 and may include additions in the following areas:

- Standardisation of information fields transmitted from the merchant to consumer, such as, purchase amount, receipt information, package tracking information, and other transaction and merchant relationships.

[2] RFC 2706: ECML v1: Field Names for E-commerce; October 1999.

- Additional consumer-to-merchant fields, such as, additional payment mechanisms.
- Improved internationalisation.
- Integration with privacy standards.
- Standards for exchange of ECML data using XML.
- Investigate standards in the wallet activation area.

ECML is publicly available and may be used with any payment mechanism. It simply allows a merchant to publish consistent simple web forms. Furthermore, it can be used with both the SSL and the SET security methods. When using ECML with the security protocol SET, the consumer has control and convenience during online shopping on the Internet.

Digital wallets, using the ECML standard, will allow consumers to store billing, shipping, and payment information and to use this information to automatically complete a merchant form.

Computer companies signing on to the standard include IBM, Compaq, Microsoft and Sun Microsystems, along with online service provider America Online. In the retail area, MasterCard, Visa and American Express, all announced the support for ECML, along with online merchants, such as, Dell Computer, Beyond.com and Healthshop.com.

6.4 Electronic Cash

Electronic cash (e-cash) also called **digital cash** is **digital money** that provides private customers with a safe, fast and low-cost means of payment in the Internet. The term "digital cash" defines a category of electronic payment systems that attempt to replicate the benefits of cash in the offline world [136]. Created by lots of individual parties, it moves through multiple networks instead of the current bank system and is best suited for micropayments.

Some of the opportunities for micropayments include the following:

- Builds truly global markets. The idea of selling inexpensive products and services opens a world of options for content providers.
- Allows cheap and flexible marketing.
- Low-cost distribution of services.
- Automation of customer interaction.

Apart from the opportunities that exist for micropayments the risks of micropayments include:

- Crypto failure.
- Lack of legal framework.
- Low level confidence, as micropayments are still in the beginning stage.

Public-key cryptography and digital signatures make e-cash possible. Both banks and customers would have public-key encryption keys. Public-key encryption keys come in pairs. A private key known only to the owner, and a public key, made available to everyone. Banks and customers use their private keys to encrypt (for security) and sign (for identification) information and/or data that represents money orders. Therefore, the bank will "sign" the money orders using its private key. The customers and merchants verify the signed money orders using the bank's widely published public key. In the same way, customers' sign deposits and withdraws using their private key and the bank uses the customer's public key to verify the signed withdrawals and deposits.

A special feature of cash, rendering it particularly desirable for the Internet, is its **anonymity** - the lack of any information on the one paying, both vis-à-vis the payee and the banking institution issuing the money. Apart from providing anonymity, electronic cash should be spent only once, should be independent on any network or storage device and should be portable. The electronic cash units and their values can be defined independently of real currency.

6.4.1 How does E-cash work?

Both the merchant and the customer establish e-cash accounts at the issuing bank, which issue tokens[3] to their customers. A customer installs a "cyberwallet" onto his computer, which will store the money requested from the bank [136]. When a customer requests for money he sends an encrypted message to the bank, which will debit the user's account accordingly. The electronic coins holding a serial number are encrypted and signed by the customer's bank before sending them to the customer. The merchant presents these to the bank for payment to verify that these coins have not been spent already once. The issuing bank keeps an online database of issued bank notes and compares them with notes presented for payment in order to find a match between the notes. The coins are marked with a unique serial number and can be used in conjunction with only one transaction.

When the consumer contacts the bank in order to withdraw electronic cash, the bank verifies his identity, issues the amount of electronic cash and at the same time deducts the amount of cash from the consumer's account. The electronic cash can only be spent on sites that accept the electronic cash for payment. When the goods are shipped to the consumer, the merchant can present the electronic cash to the bank, which will then credit the merchant's account for the transaction amount. Of course the electronic cash must be protected in order to avoid some of the disadvantages, such as, double spending and forged cash.

In e-cash transactions the payee does not know the payer's identity. On the other hand the issuing bank may or may not keep the identity of the recipient of the electronic bank notes, which is not satisfactory. Whereas the customer is to remain anonymous both vis-à-vis the merchant and the bank, it is necessary to ensure that the bank cannot read the serial number when signing the coins. This can be prevented by means of the so-called "blinding" technology. The payee can check the authenticity of the coins by means of the bank's electronic signature.

[3] A token is an electronic object with a unique encoded serial number and an encoded digital signature of the issuing bank.

6.4.2 Types of E-cash

There are two *distinct types* of e-cash:

- Identified e-cash
- Anonymous e-cash (will be illustrated below using the DigiCash's model)

Identified e-cash contains information revealing the identity of the person who originally withdrew the money from the bank. The identified e-cash can be tracked back as it moves from one person to another, which does not hold for **anonymous e-cash**. Once anonymous e-cash is withdrawn from an account, it can be spent or given away without leaving a transaction trail. Anonymous e-cash is created using blind signatures rather than non-blind signatures.

There are two *varieties* of each type of electronic cash: online e-cash and offline e-cash, meaning electronic cash can be held online or offline. When the cash is held **online**, a bank is involved in the transfers of electronic cash and the consumer does not personally have possession of the electronic cash. **Offline e-cash** means a transaction is conducted without having to directly involve a bank and the customer does have physical control of the electronic cash. This is what makes offline the most complex form of e-money because of the *double-spending* problem.

The double-spending problem occurs when a piece of e-money can be copied and both copies can be spent. Since e-money is just a bunch of bits, a piece of e-money is very easy to duplicate. To avoid double spending serial numbers can be attached to the electronic cash, but electronic cash with a serial number is no longer anonymous.

Online e-money systems prevent double spending by requiring merchants to contact the bank's computer with every sale. The bank's computer maintains a database of all the spent pieces of e-money and can easily indicate to the merchant whether a given piece of e-money is still spendable. The merchant can then refuse the sale if the bank confirms that the piece of e-money has already been spent.

6.4.3 Strengths and Weaknesses of E-cash

Achieving the advantages and disadvantages, listed below, depends on every payment system individually. Some of the general advantages to use electronic cash are:

- *Anonymity*: Digital money offers the possibility of secure anonymous payment via the Internet.
- *Privacy*: E-cash is untraceable, which ensures a great deal of privacy. As the bank does not link the serial numbers to a particular person it is impossible to link payment to payer.
- Allows for *micropayment* (i.e. extremely small sums) on the Internet and provides lower transaction costs than other electronic payment systems.
- The distance, which e-cash must travel in a transfer does not effect *the transmission costs* or *travel time* as it does with traditional payment methods.
- Banks that issue e-cash could find it much *cheaper* than handling cheques and the paper records that accompany traditional money. This could make e-cash more convenient, efficient and flexible than traditional money.
- Electronic cash will let businesses carry out transactions *around the world* without transferring bank funds and they will be able to reach a *large population of consumers*.
- Because e-cash is basically software, it can be *programmed* to do things that paper money could never do.

The disadvantages of electronic cash are not insignificant. They include the following:

- A third party must create electronic cash and both customer and merchant must use the software. This means *additional software* must be installed and learned.
- *Double spending*, meaning the cash can be spent twice by submitting it to two different vendors.
- Electronic cash is difficult to trace and therefore, raises the important question of *taxation*. With e-cash, the merchant could be in South Africa and the buyer in Germany, while the sellers' computers are located in Canada. The question is whose sales tax must the seller pay?

- Since e-cash does not leave an audit trail, it could be used in *money laundering* operations or as a medium of exchange in other illegal activities. Therefore, criminals can use untraceable cyberdollars to hide assets offshore.
- Spent electronic cash can be *forged*. Own personal mints of e-cash can be created, which would be indistinguishable from real money.
- Uncontrolled growth of e-cash systems could *undermine bank- and government-controlled money systems*.
- Money stored on a PC could be *lost* forever if the system crashes. Therefore, e-cash may be less secure than bank money. Furthermore, if computer hackers or other criminals were to break into e-cash systems, they could change the electronic wealth of thousands or even millions of innocent consumers.

Apart from all the disadvantages e-cash also raises some questions, such as: Who should be allowed to issue e-cash, and who will regulate those issuers? How will taxes be applied in cyberspace, which cross physical boundaries? Who will set the standards? How do you ensure that payments made over the Net will be secure? How will consumers be protected? How will regulators police money laundering and counterfeiting on private networks?

6.4.4 The eCash (DigiCash) Payment System

DigiCash [124], founded by **Dr. David Chaum**, filed for bankruptcy in **November 1998** [24], [104]. DigiCash was to become the most prominent force in the electronic cash battle. The eCash coins have been available on the Internet since **October 1995**, when the Mark Twain bank of St. Louis, Missouri, started issuing them [79]. However, when the Mark Twain Bank dropped the coin offering in **September 1998** [122], DigiCash suffered a setback. In **1999** eCash Technologies Inc. acquired the DigiCash properties and offers now secure and *anonymous* cash-like electronic payments [167].

The eCash product, a coin-based digital money system is momentarily the only practicable system capable of ensuring the payer's absolute anonymity. Strong security is provided using *asymmetric* and *symmetric cryptography* [79].

The problem facing coin-based systems is that digital coins can easily be copied any number of times. This makes it essential to incorporate some way of ensuring that digital coins can be used only once. The method employed is that of assigning *unique serial numbers*, which are registered in a special database, to the coins.

6.4.4.1 Anonymous Digital Cash by DigiCash

Dr. David Chaum argues that although digital signatures are secure they do not provide any privacy. As a result of this he has developed a cryptographic invention known as **"blind signatures"**, as a means of implementing anonymous digital cash [31].[4] The blind signatures are an extension of digital signatures that can restore privacy. This technology uses electronic cash with embedded serial numbers and which the bank digitally signs. David Chaum's primary goal with his form of electronic cash was to ensure privacy protection and that it operates as anonymously as traditional cash.

The eCash system uses the blind signature technology to provide anonymous cash tokens, with a specific technique that will detect *double spending* and at the same time identify the perpetrator.

6.4.4.2 How does the eCash system work?

Both the consumer and the merchant must have an account at the eCash bank [129]. Consumers withdraw electronic coins, of various denominations at an eCash bank, via credit card or wire transfer, in order to make payment at a later stage. These coins are generated involving the blind signature scheme to make the tokens anonymous. The

[4] A digital cash system is blind or anonymous if the bank is unable to determine, which coin was withdrawn by which user.

tokens can be used just like real cash and are stored on the consumer's hard drive in their eCash wallet. The encoded signature serves as a check against unauthorised duplication.

When a client withdraws coins from the electronic bank, the amount needed is entered in the client's cyberwallet [79] software. The client's wallet software generates random serial numbers for each bill, usually with a 100-digits serial number [129]. The serial numbers of the coins are then "blinded" by multiplying the coins' unique numbers by a random factor (i.e. blinding factor). A customer digitally signs the serial number with his private key corresponding to the public key that he has previously established for use with the account and sends it to the bank. Before sending, the whole request is protected by encrypting it with the bank's public key. Using the public key, the bank verifies the customer's digital signature and removes it from the note number. The bank blindly signs the serial number on the coin with a private key and debits the amount to the customers account.

After the customer receives the blinded note signed by the bank, he/she decrypts the message, unblinds the coins (i.e. takes out the blinding factor) and spends the coins whenever needed. Because the bank, upon signing the serial number on the coin, has no idea of the blinding factor used on the coins (i.e. it is prevented from seeing the serial number of the coins), it is unable to trace the blinded serial number and will have no idea of who spent the money. In this way, full anonymous electronic cash is provided to the payer. This anonymity, however, gives rise to the problem of double spending.

When the merchant receives an order, he sends a payment request to the client's cyberwallet, which will present the user with the information and subsequently ask him if he wants to make a payment on the net. The user confirms the amount, purpose and payee, encrypts a sum of the DigiCash with the bank's public key and then the eCash software transfers the *exact* value in coins from the user's disk to the merchant over the network. The merchant will check with the minting bank if the coins are valid, who will then deposit the tokens into the bank account of the merchant in order for the merchant to

receive "real" currency in return. Figure 6-1 shows an overview of the eCash payment system.

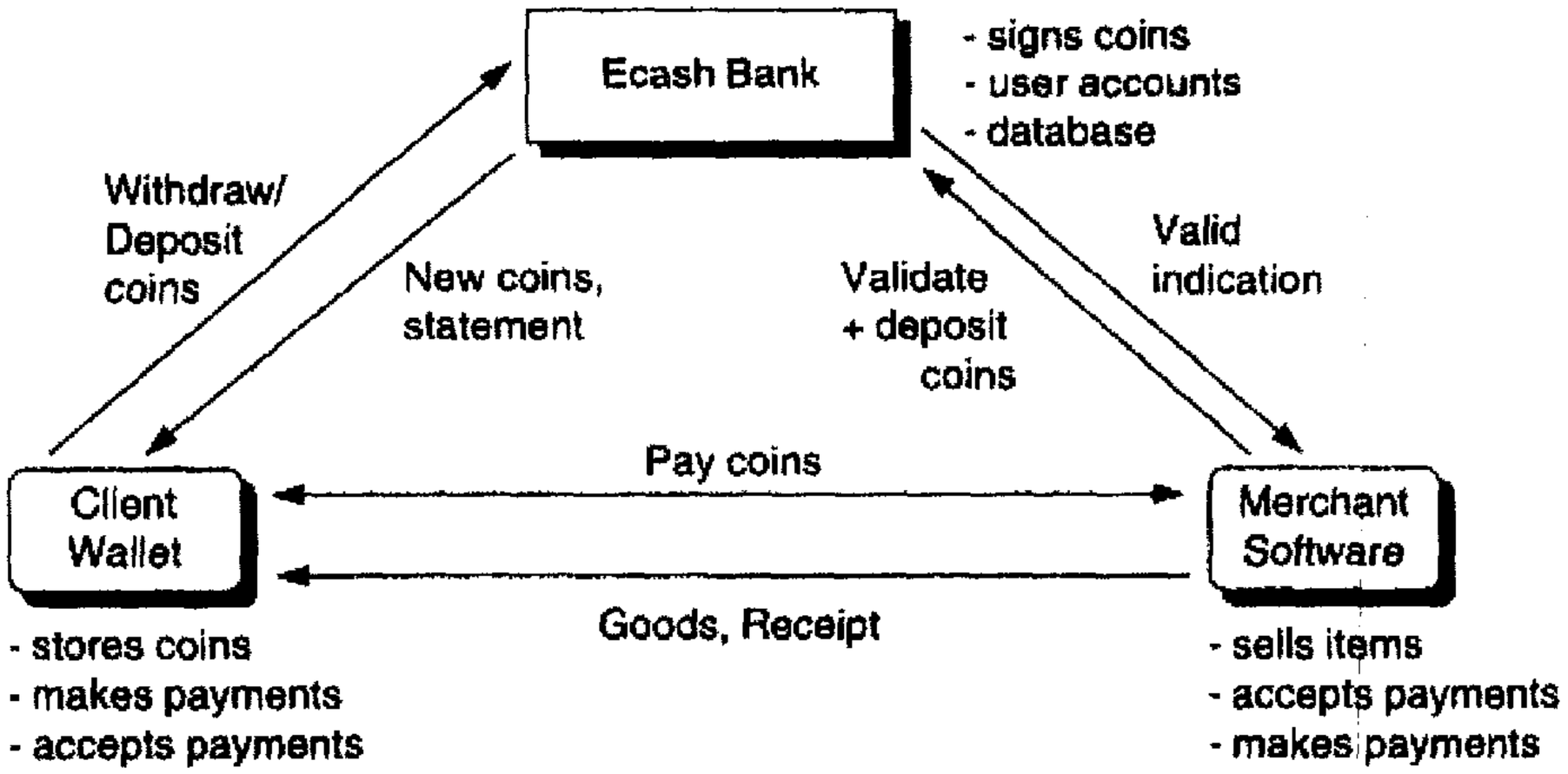


Figure 6-1 Overview of the eCash Payment Model (Source: [79])

6.4.4.3 Double-spending prevention

As concluded from above, blinded electronic bank notes protect an individual's privacy. However, since the bank cannot see the serial numbers on the coins it issues, these coins cannot be recorded [79] when issued to a customer. Furthermore, each eCash coin is simply a number, looks alike and can be easily copied, making it impossible to detect double spending. To overcome this problem the eCash can include a serial number and the merchant can check, upon receiving of the digital cash from the customer, with the bank whether the cash has come from the bank. At this stage the bank verifies, using the encrypted serial note number, whether somebody else has already deposited cash with the same serial number (double-spent) [123]. The serialised coins are checked online against the bank's database (i.e. a central list) of all serial numbers ever spent. If there is no match and the coins hold the bank's signature, they are valid. After successful verification, the value of the coins are credited to the merchant's account and the coins are destroyed while the serial numbers are added to the database of spent coins to prevent

double spending. A signed receipt is returned to the buyer's cyberwallet from the merchant. This type of digital cash is however not anonymous.

To solve this problem, David Chaum proposed a method for generating blinded notes that requires the payer to answer random numerical queries about each note when making a payment. Spending such a note once does not compromise unconditional untraceability, but spending it twice reveals enough information to make the payer's account easily traceable. In fact, it can yield a digitally signed confession that cannot be forged, even by the bank.

Therefore, in Chaum's approach, using serial numbers, one can't identify the client to whom a certificate was issued even if all parties collide. However, a client attempting to spend the same certificate twice provides enough information to determine his identity.

6.4.4.4 Advantages and Disadvantages of the eCash system

The advantages of the eCash system are:

- Fully anonymous [79] and untraceable digital cash.
- Ensures double-spending detection.

The disadvantages of the eCash system are:

- A bank account at one of the issuing banks is required.
- Graphical wallet software is required.

The eCash system was initially trialed on the Internet and introduced cash in cyberspace using CyberBucks or DigiCash coins. These coins cannot be directly exchanged to real money, but are only used when users purchase goods and services on the Internet.

6.4.5 The CyberCoin Payment System

CyberCash, Inc., [120] provides a range of solutions for all types of Internet payments. Their payment products include CyberCash the credit card based payment system (which will be discussed under 6.6.3), CyberCoin the electronic cash payment system and PayNow for cheques. Using PayNow, customers can make payments to CyberCash directly from their check accounts [92].

The CyberCoin [121] system is designed for micropayments [123], ranging from 25 cents to 10 USD [92]. For a real micropayment system 25 cents is however still too much. Currently the CyberCoins are only available in U.S. dollars and to merchants who have an U.S. bank account. CyberCoin implements a notational system and not a token system.

6.4.5.1 How does the CyberCoin system work?

Using this cash system customers rely on their existing bank account for any CyberCoin transaction. The CyberCoin wallet is downloaded from the CyberCash server using a credit card or bank account. Once downloaded, the wallet is used to store the CyberCoins (i.e. tokens). Upon obtaining CyberCash from the server an account is established with the CyberCash server.

Before using CyberCoin to pay on the Internet, the electronic wallet must be "charged". If a customer wants to fill his wallet, money is transferred from the customer bank account to the CyberCoin account at CyberCash supporting bank. The customer does not store any monetary value on its PC.

When a user wants to a make payment he authorises the CyberCoin supporting bank to transfer an amount from his account to the merchant's account. The merchant will verify this payment with the CyberCash server. The CyberCash server acts as a middleman, transferring funds between the user account and the merchant. In this way no monetary value ever leaves financial networks. Although the merchant will not know the

customer's identity, the server has a record of each user's transaction. Figure 6-2 shows the steps in a transaction using the CyberCoin payment system.

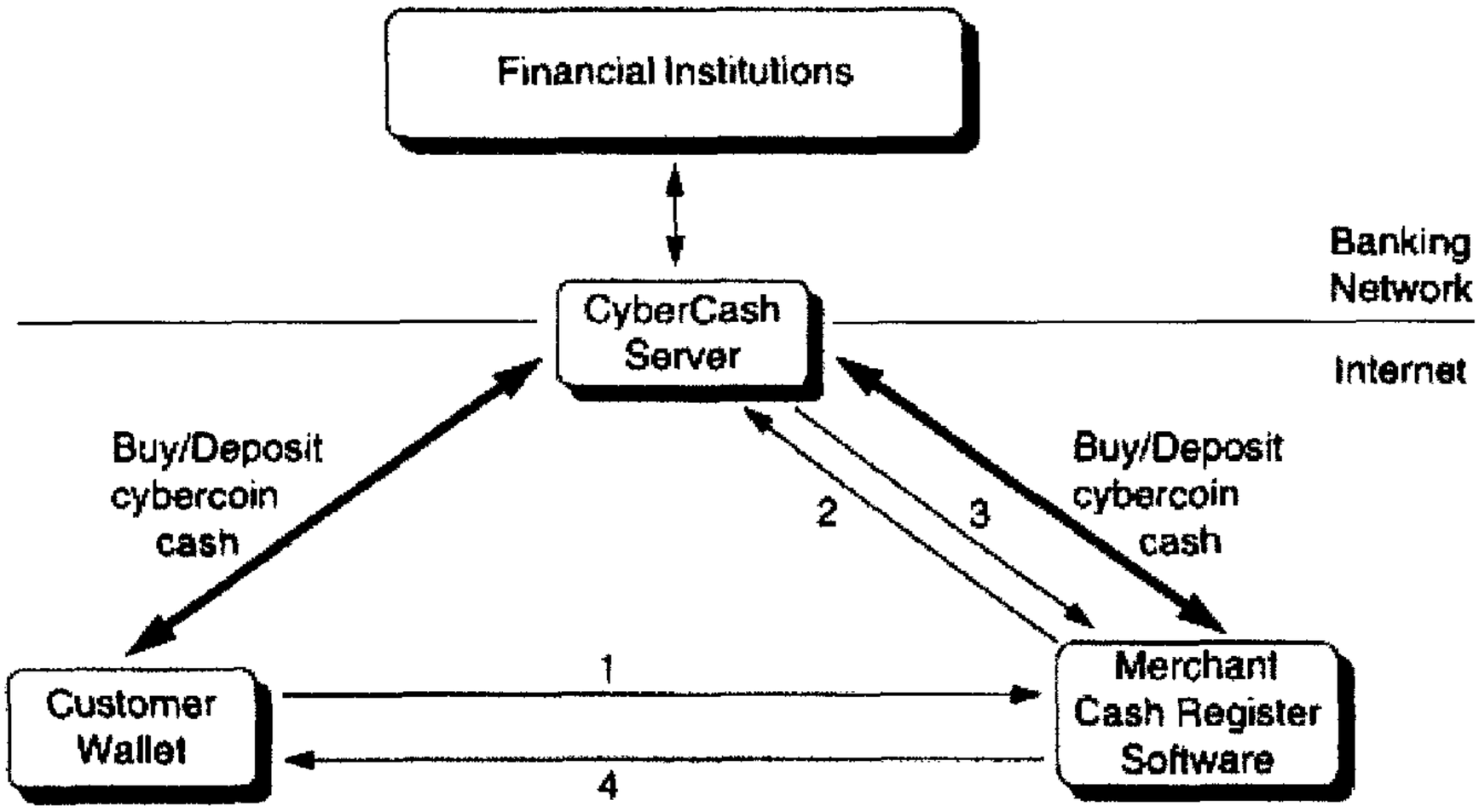


Figure 6-2 Use of CyberCoin Payment System in a transaction (Source: [79])

6.4.5.2 Advantages and Disadvantages of the CyberCoin system

The advantages of the CyberCoin system are:

- U.S. citizens can bind their bank account to the wallet software [129].
- The customer never holds monetary money, so it cannot be lost (by, for instance, a hard disk crash) or stolen.
- The customer is protected from loosing money. The wallet will release CyberCoins to the merchants only after the customer has received the goods.

The disadvantages of the CyberCoin system are:

- The CyberCash wallet software is required.
- Merchants need an U.S. bank account and will be charged a transaction fee.
- For non-U.S. citizens a credit card is necessary [129].

CyberCoin has been operational since **1996**, but as of **April 1999** [67], CyberCash has closed CyberCoin accounts [24], [167], [104]. The company refocused its small transaction value business in its new product called **InstaBuy** [140]. InstaBuy uses, as CyberCoin, a direct account based payment model with online validation. InstaBuy works similarly to other e-wallets, except that no software needs to be to downloaded and any personal information is stored on the CyberCash encrypted servers. The user needs to enter his payment and shipping data only once. This data will be re-used at every visit to an InstaBuy enabled merchant [158]. When signing up for an InstaBuy account, a password is chosen that is only known to that person. InstaBuy makes use of the standard Secure Sockets Layer (SSL) technology [104] and 128-bit encryption.

6.4.6 The NetCash Payment System

NetCash is a real-time, cash-like electronic payment system being offered by the **NetBank**, and is designed to support mainly information products under $100 but can be used for payments as low as $0.25 [60]. It consists of multiple currency servers that issue the coins to users, allowing users to choose the server most appropriate to them. NetCash provides scaleable electronic currency that is accepted across multiple administrative domains without requiring the use of tamper-proof hardware.

NetCash will use the NetCheque system to clear payments between currency servers and at the same time allow clients to buy and sell coins in exchange for electronic cheques. Therefore, all the cheques can be cleared through the NetCheque clearing infrastructure.

6.4.6.1 How does the NetCash system work?

A customer must first set up an U.S. checking account in order to buy NetCash coins of exact denomination [60]. Coins are purchased from a currency server (i.e. NetBank) by sending U.S. dollars or electronic cheques, encrypted with the server's public key the server, in exchange for NetCash coins. Each coin is minted by the currency server and consists of a unique serial number with an exact value. Before sending the coin to the

customer, the coin is encrypted with the minting server's private key. This forms a digital signature to show that it is authentic. The user in exchange receives a bill, sent by an encrypted e-mail, including the following information:

- The "NetCash U.S.$" keyword,
- The dollar amount, and
- The serial number of the bill.

For example: NetCash US$ 50.00 A3456374633866353.

When a customer wants to make a purchase he/she is sending a purchase request to the merchant encrypted with the merchant's public key. The customer first needs to send his public key to the merchant. The merchant can then use the public key of the customer to encrypt his public key before sending it to the customer. For payment the customer is e-mailing the serial number and the coins, in exact value, to the merchant. Upon receipt of a NetCash bill, the merchant verifies the signature on the coins using the server's certificate. Furthermore, he sends the serial number to the currency server, or directly to the minting server, for verification. A currency server maintains a list of serial numbers of every coin issued and all the coins redeemed are removed from the list of issued coins. For verification, the currency server checks that a coin's serial number is present in its database. If it is present, then it is a valid coin originating at the server and NetBank will "accept" the bill. The serial number is then deleted immediately from the list of issued coins and the coin is automatically exchanged for a new one with a different serial number. This *prevents double spending* since once a bill is used it is permanently removed from circulation. However, if the serial number of the coin is not present in the list then the coin is not valid with respect to the server in question. The NetCash payment system is shown in Figure 6-3.

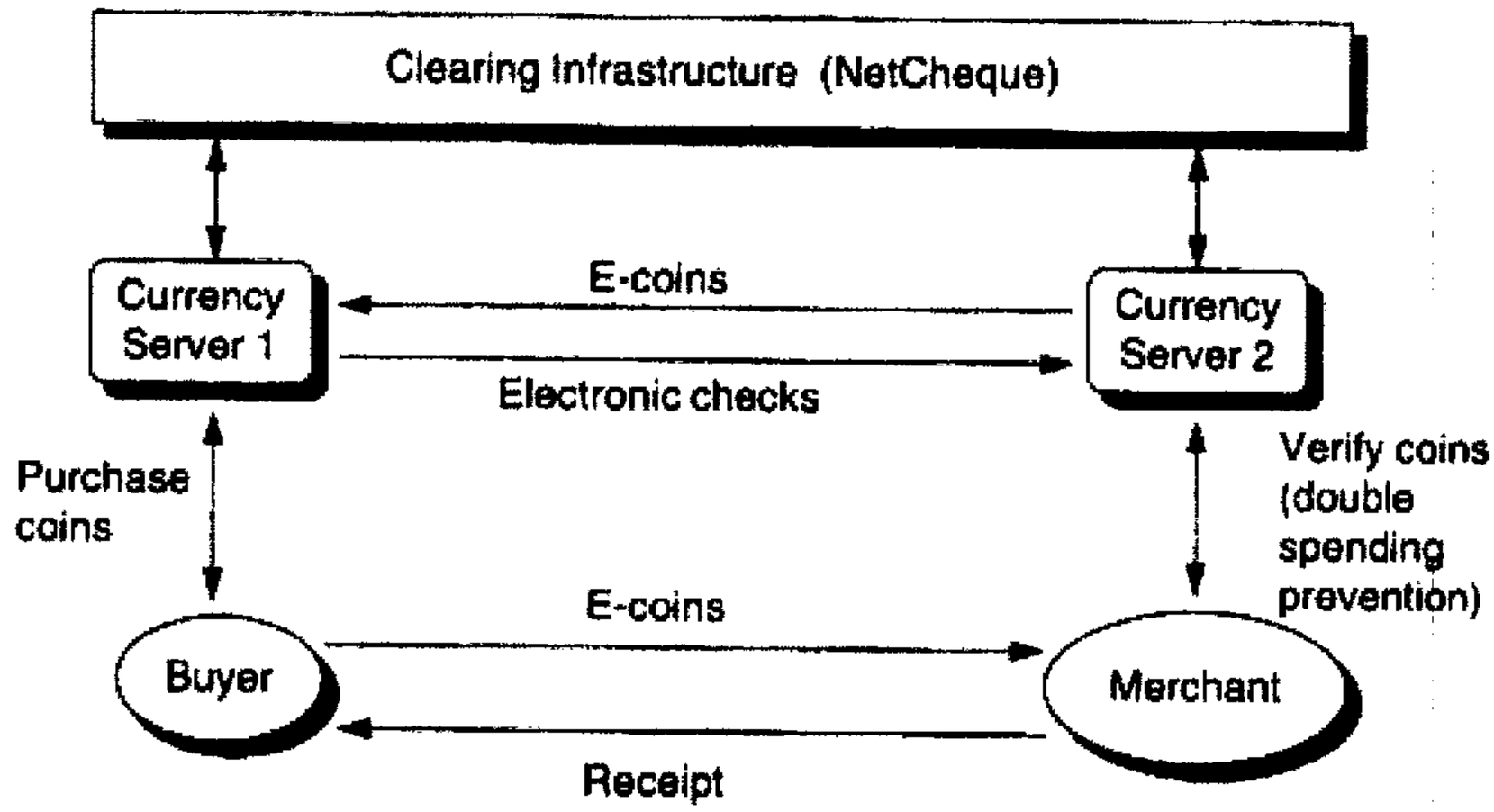


Figure 6-3 Overview of the NetCash Payment System (Source: [79])

6.3.6.2 Advantages and Disadvantages of the NetCash system

The advantages of the NetCash system are:

- No penalty is incurred if the customer or the merchant keep the NetCash in the "online world" (such as, using it for the purchase/sale of other goods and services) [60].
- NetCash offers a "change" function where the customer or the merchant can have their loose bills and change consolidated into higher denominations.

The disadvantages of the NetCash system include:

- Every customer must set up an U.S. checking account.
- The transaction is only anonymous with the consent of the currency server.
- Exact change is required in carrying out sales transactions, which while automated is a hassle. Therefore, transactions are very cumbersome.
- If the customers have a lot of spare change, the NetCash system can become difficult to maintain.
- The use of e-mail is not always very convenient.

For security reasons, NetBank customers and merchants are encouraged to use data encryption algorithm, such as, Pretty Good Privacy [151] on their e-mail messages.

6.4.7 The MilliCent Micropayment System

Digital Equipment Corporation (DEC), which is now part of Compaq [92] created MilliCent [142] as a micropayment scheme. The key innovations of MilliCent are its use of brokers and of scrip. *Scrip* is digital cash that is merchant or vendor specific, i.e. valid for one particular vendor only. It enables payment of values under $5, including amounts as low as a tenth of a cent ($0.001) [44], to be made. *Brokers* take care of account management, billing, connection maintenance, and establishing accounts with vendors. MilliCent principally aims at content providers, who are looking for ways of charging users on a pay-per-use, rather than subscription basis.

6.4.7.1 How does the MilliCent system work?

MilliCent, an electronic scrip system, allows merchants to generate their own currency, called "scrip" in order to sell it to a broker at a discount. The brokers, acting as intermediaries between vendors and customers, are distributing different vendor scrip to the customers and maintain accounts of customers and vendors. The fact that any type of scrip is only valid at a particular vendor means the vendor does not need to connect to a central issuer to validate the token [129]. Because of the broker, a customer does not need to deal with many brokers in order to obtain scrip for many merchants, meaning all the different vendor specific scrip can be obtained at one broker.

Figure 6-4 shows the MilliCent payment process. The customer first buys some broker scrip, which is stored on the customer's computer in an electronic wallet. Before making a purchase on the merchant's web site, the customer needs to convert the broker scrip into vendor-specific scrip. The broker obtains the required vendor scrip from the vendor.

At the time of purchase the vendor-specific scrip and the purchase request is sent to the vendor. The vendor locally validates the scrip to prevent customer fraud and to ensure himself that the scrip is [79]:

- Authentic scrip produced by the vendor or licensed broker, and
- Not spent already.

To prevent *double spending* the vendor compares the unique identifier of the scrip (presented as an ID number) obtained from the customer with the list of spent scrip ID numbers maintained by the vendor. After the MilliCent vendor or merchant receives payment he sends the scrip to the broker in order to obtain a cheque.

The fact that the vendor can validate the payment without involvement of a third party keeps the per-transaction costs very low and makes MilliCent a suitable micropayment system. In this way the network traffic is reduced tremendously [129].

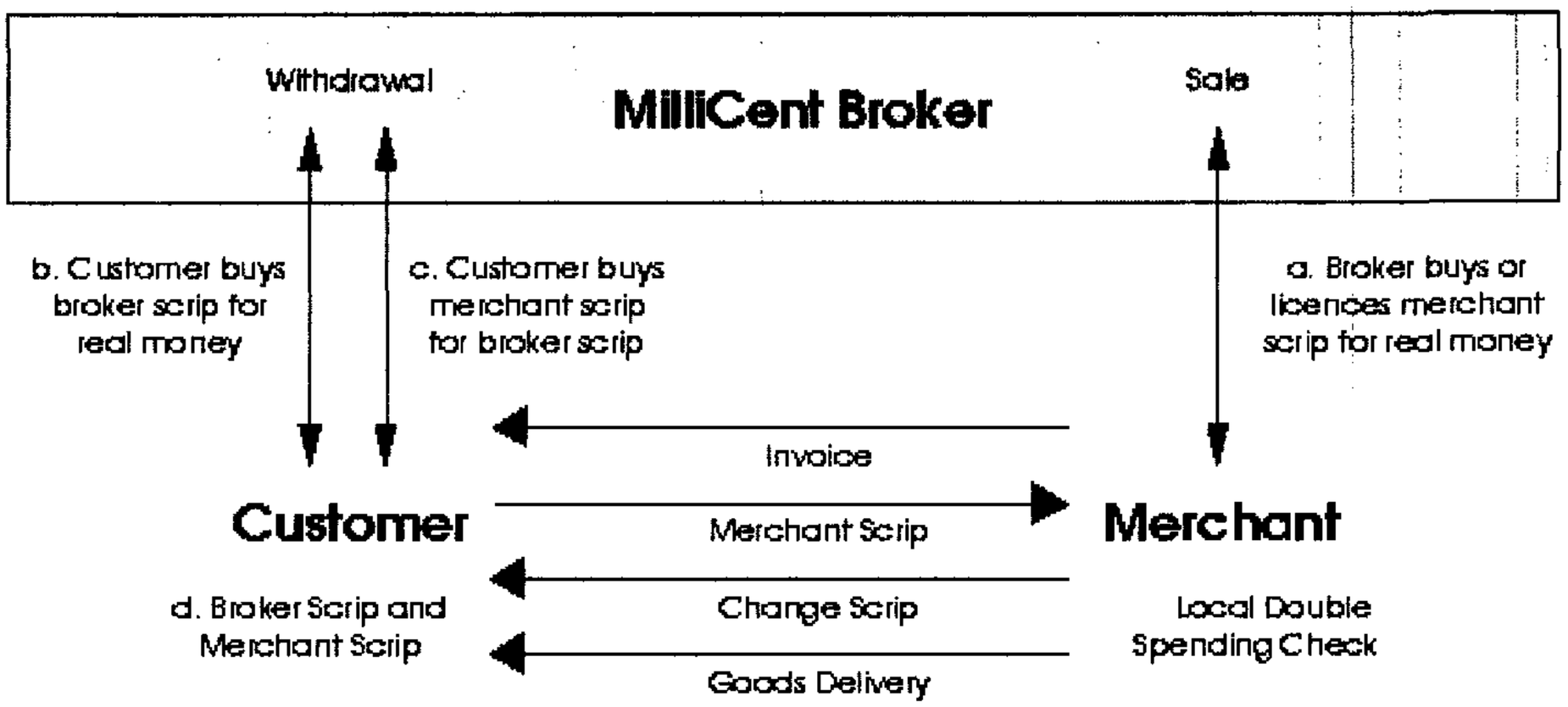


Figure 6-4 Overview of the MilliCent Payment Model (Source: [129])

6.4.7.2 Advantages and Disadvantages of the MilliCent system

The advantages of MilliCent are:

- Allows real micropayments (especially when compared to the above three payment systems).
- Fast cheap light protocol.

- A choice between many brokers exists in order to buy the scrips.
- The broker has only restricted knowledge about the buyer and the deals.

The disadvantages of MilliCent include:

- Provides no anonymity [123].
- Requires special understanding of the scrip model and complex business architecture.
- The scrip is being vendor-specific, which could lead to scrip leftovers that cannot be used at other sides.
- Holds no relation to other payment systems.

MilliCent may also be used for different purposes than micropayments, like authentication, metering, usage-based charges and discount coupons. The performance of MilliCent is satisfactory - it can keep up with the arrival of transactions over the network.

6.5 Electronic Cheques

Electronic cheques are the equivalent of paper-based cheques. Although the paper-based cheque system is very expensive to process, there is still a need for a cheque-based payment system that transfers funds from the payer's bank to the payee's bank. The electronic cheque system works exactly in the same way as the paper-based system, except, that the cheques are initiated during an on-screen dialog and the funds are transferred over a computer network at the time of the transaction. Authentication and verification are performed instantaneously by using digital signatures and timestamping controls during the transaction [48]. According to Greenstein [36, page 313] the web-based electronic cheque payment system performs the following functions:

- Presents the bill to the payer.
- Allows the payer to initiate payment of the invoice.
- Provides remittance information.
- Allows the payer to initiate automatic payment authorisations.
- Interfaces with financial management software and transaction processing software.

- Allows payments to be made to new businesses with which the payer has never transacted before.

These functions have the advantage that the payer does not need to visit the payee's web site in order to retrieve the bills, but he can retrieve the bills by e-mail from the payee.

6.5.1 The Financial Services Technology Consortium (FSTC) Electronic Check Project [5]

The electronic check (eCheck) project [125] is a cheque-like payment system, developed by the **Financial Services Technology Consortium** [131] as part of the Bank Internet Payment System (BIPS), [6] to pay merchants. It is an electronic version of a paper cheque, which contains sufficient information necessary to process a payment (i.e. complete a transaction) without the intervention of an authorising financial institution. The electronic equivalent of the signature will be implemented via *digital signatures* from a smart card-based device. *Digital certificates* will be used to authenticate the payer, issuer and bank account.

The Financial Service Markup Language (FSML) was used as the mark-up language to write and structure the eChecks that contain all the information also found in a paper cheque. The FSML is a block of structured data description language based on SGML [125].

Overall, the FSTC eCheck is comparable to Mondex, also requiring the consumer to possess a smart card reader. Using the FSTC electronic check, it will be possible to produce a variety of different payment types, such as, electronic charge cards, certified cheques and travellers cheques.

[5] When referring to the FSTC electronic check project, the spelling "check" instead of "cheque" (as used throughout the rest of the document) will be used.
[6] See Internet Page at URL: http://www.fstc.org/projects/bips/

6.5.1.1 How does the FSTC eCheck system work?

Authorised individuals are assigned a portable electronic checkbook in the form of a secure hardware device. The electronic checkbook smart card stores and delivers the customer's private-key and certificate information for signing the checks, as well as, a list of all the checks being generated. Payments are collected via e-mail and cleared through the existing financial networks.

Figure 6-5 shows the payment model of an eCheck. The payer writes the eCheck on a computer, cryptographically signs it, and e-mails it via the Internet. The payer signs the eCheck using the secure hardware device, and includes its authenticating certificate, signed by the issuing bank The payee receives the eCheck, verifies the payer's signature on the eCheck, endorses it, writes a deposit slip, and signs the deposit slip. The endorsed check is then sent by e-mail to the payee's bank for deposit. The payee's bank personnel verify the payer's and payee's signatures, credit the deposit, and then clear and settle the endorsed eCheck by sending it to the payer's bank. The payer's bank verifies the payer's signature once again and the amount on the eCheck is debited from the payer's account.

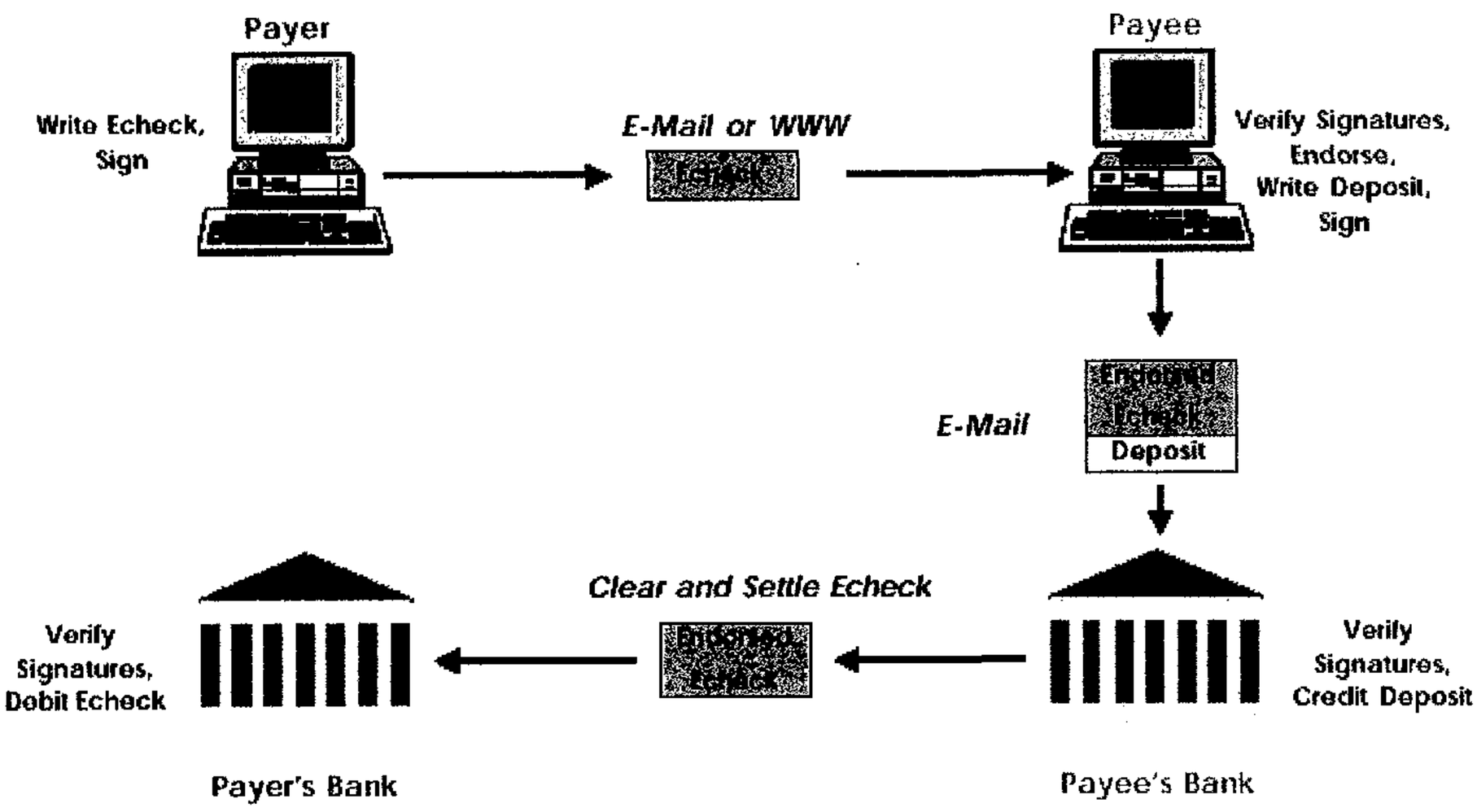


Figure 6-5 Payment model of eCheck (Source: [125])[7]

[7] Article by Anderson Milton M., The Electronic Check Architecture, version 1.0.2 – September 29, 1998.

When the payer issues a check, he grants his bank to make a payment to an identified payee by transferring the funds from the payer's account to the payee's account over a computer network. Any payer who issues a check has enrolled in some kind of public-key-based identity scheme.

Since the eChecks are designed to be compatible with existing financial networks, any bank would honour them and they can be cashed in by anyone at any financial institution. However, for a customer to "write" electronic checks, they require a smart card reader.

6.5.1.2 Scenarios supported by the FSTC eCheck system

The eCheck can support a number of data flows. The FSTC has identified four such payment scenarios or functional flows [130]:

- The *deposit and clear* scenario requires both parties to have processing capabilities to deal with eChecks. The payer issues an eCheck to the payee who will endorse the eCheck and then forward it to his bank. The bank, in turn, settles the eCheck with the payer's bank.
- In the *cash and transfer* scenario the payee's bank cannot accept cheques electronically. The payer issues an eCheck and sends it to the payee. The payee present the eCheck directly to the payer's bank (instead of this own bank) to be paid to the payee's account at his bank.
- Using the *lockbox* scenario the eCheck is sent either directly to the payee's primary bank account or via a lockbox. A lockbox is a special purpose account held by a third party on behalf of the payee. The payee's bank notifies the payee and clears the eCheck with the payer's bank.
- The *funds transfer* scenario requires only the payer's bank to be equipped with processing capabilities for electronic checks. The payer issues an eCheck to its bank. The payer's bank will then transfer the funds to the payee's bank account at the payee's bank.

6.5.1.3 Advantages and Disadvantages of the FSTC eCheck system

The advantages of the eChecks are:

- They work like a paper cheque but only in pure electronic form, with fewer manual steps.
- They are based on the same rich legal framework as paper cheques [125].[8]
- The eChecks utilise state-of-the-art security techniques of authentication, public key cryptography, digital signatures, certificate authorities, duplicate detection and encryption.
- Validation is done online.

The disadvantages of the eChecks include:

- Merchants assume all risks for bounced cheques and they do not receive immediate payment.
- Non-anonymous transactions [125].
- The system is expensive for merchants, as it is not totally net-based.

Due to customers' familiarity with the traditional cheque mode, and the use of existing, trusted financial institutions [123] for the eCheck, it is expected that the FSTC eCheck project will promote fast customer acceptance.

6.5.2 NetCheque as an Electronic Cheque Payment System

Another cheque-like system, supporting the debit electronic payment model, is the NetCheque payment system. NetCheque [148], developed at the **Information Sciences Institute of the University of Southern California**, is a *distributed accounting service* to represent and process electronic financial instruments similar to cheques.

The NetCheque system is seen as complementary to NetCash. One of its suggested uses

[8] Based on the article *eCheck: Overview: What is eCheck?* at URL: http://www.echeck.org/overview/what.html

is to clear cheques between servers of different types. For creating signatures and endorsing cheques *symmetric key encryption* is used (based on the Kerberos tickets), in contrast to the public key systems used by other cheque-based systems, such as, the FSTC eCheck system [123]. The requirement for handling micropayments requires high performance, which is obtained through the use of conventional crytography instead of public-key cryptography. Symmetric keys are faster, and therefore, more suited to micropayment systems.

Users of NetCheque maintain accounts on accounting servers of their choice. Once registered with NetCheque accounting servers they 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.

6.5.2.1 How does the NetCheque system work?

NetCheque works in much the same way as paper cheques, with the account holder issuing an electronic document that contains the amount of the cheque, unit of currency, expiry date, the payer's account number, the name of the payer, the name of the financial institution, and the name of the payee. Most of the information is in non-encoded form. The bank against which the cheque was drawn must however verify the signature of the payer.

To issue a cheque the system obtains a *Kerberos ticket* to authenticate the payer to his bank and adds a cheque-sum, which is placed in the signature portion of the cheque (i.e. in the authenticator) [123]. The signed cheque is encrypted using the session key, which the user shares with the bank, and then appended together with the ticket to the cheque [79]. The whole cheque is then sent to the payee via e-mail or online. To deposit a cheque the payee must obtain a Kerberos ticket for the customer's bank from a Kerberos server to authenticate himself and to ensure that the cheque can only be paid into his account

[123]. The payee then sends the cheque to his bank, which may be cleared by the servers in real-time or batch processed. Therefore, like a paper cheque, a NetCheque payment instrument bears an electronic signature, and must be endorsed by the payee, using another electronic signature, before the cheque will be paid. Refer to Figure 6-6, which shows the payment model of the NetCheque system.

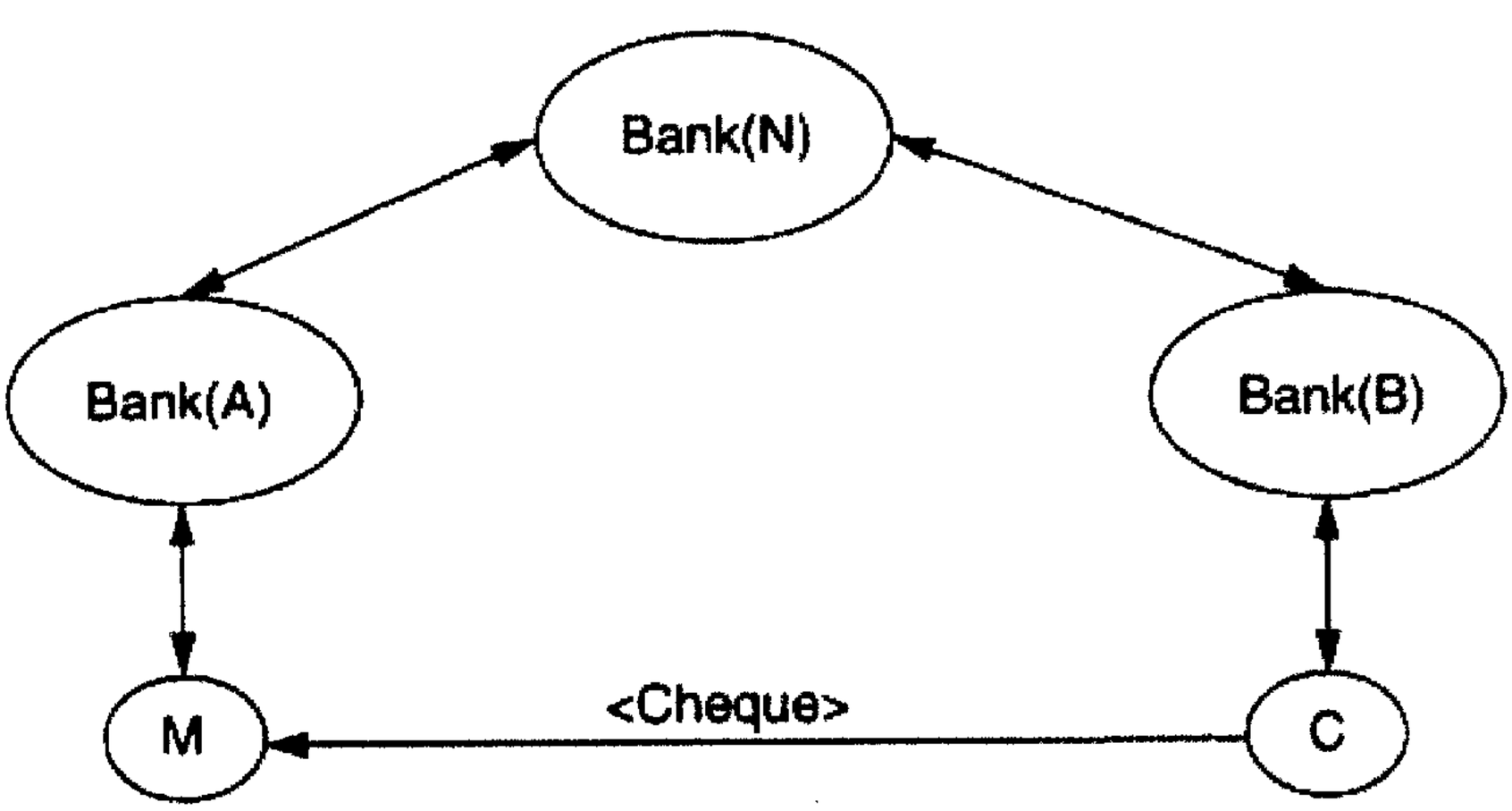


Figure 6-6 Payment Model of the NetCheque System (Source: [79])

6.5.2.2 Advantages and Disadvantages of the NetCheque system

The advantages of the NetCheque system are:

- Conventional cryptography eases the handling of micropayments.
- Signatures are authenticated using Kerberos, ensuring a great deal of security.

The disadvantages of the NetCheque system are:

- Non-anonymous transactions.
- Small initial customer base.
- Users of NetCheque must be registered as NetCheque users before they can make payments. However, once registered with one server, cheques written by the user may be cleared through any NetCheque server.

- Merchants have to bear all the risk for bounced cheques and they receive payment only after 24 hours [159].

The strengths of the NetCheque system are its security, reliability, scalability, and efficiency [75], whereas the scalability is provided using multiple NetCheque servers.

6.6 Smart Cards

Smart cards are a credit-card-sized, plastic card with an embedded **integrated circuit chip**; some smart cards being smarter than others. "Chip" being the keyword as it is exactly the chip which makes a normal plastic card "smart" and usable to serve many different purposes and applications. They are small, personal, efficient, paper-less, and a secure mechanism for offline storage of financial or transactional information. Information, such as, private codes, account details, passwords, private encryption keys or valuable personal information (e.g. ID information, house and office keys) are stored on the smart card.

Smart cards ensure *confidentiality, integrity* and *availability*. Smart cards allow users to make a purchase or exchange value and provide personal and business data only to the appropriate persons. They execute sensitive functions and support *multifunctional applications*. Offline processes, such as, public or private key encryption and decryption are performed. A multiple application card can support different types of applications (e.g., healthcare, financial services, travel, and childcare programs) on the card itself, thereby reducing the number of cards in the wallet [112].

Smart cards can be differentiated between disposable stored-value cards or personalised smart cards. As the name already indicates, **personalised smart cards** store confidential information that can be used in, for example, payment transactions. **Disposable stored-value cards** are used in applications, such as, telephone, parking and taxis. Furthermore, smart cards are divided into two categories: memory cards and processor cards. **Prepaid**

memory cards (i.e. stored-value cards) contain less information and processing capabilities than processor cards. If the memory cards have a stored value, they are called an electronic wallet. Once the value has been used up, more can be added. The cardholder of a smart card cannot tamper with the balances stored on the card and the card cannot be duplicated in any way. Smart cards holding a microprocessor are referred to as **processor cards**.

Processor cards can appear in both contact and contactless form.

- *Contact cards* hold an integrated chip that requires an external device, usually a card reader, for exchange of data. Contact cards therefore, have a visible metal contact area on the face of the card. The cards are not swiped, but inserted into a special card reader, with precise alignment between connections. This ensures adequate power for fast processing and the strong signal reduces the risk of error. But direct physical contact causes wear in the card over time.
- *Contactless cards* provide added flexibility for the user's card, as they do not require a contact with an external device but can be read from a distance. The power and data transfer is achieved through low frequency radio waves using inductive coils or high-frequency radio antennae embedded in the card. Contactless cards are more robust, reliable and longer-lasting than contact cards.

6.6.1 Smart Card Applications

The smart card usage is becoming more and more significant and will play an important role in our daily life. Three main kinds of applications of smart cards are identified.

1. *Authentication applications*. Smart cards can act as an identification card, for example a University ID card, which is used to authenticate the cardholders (in this case the student) and card readers, thus allowing cardholders to gain access to buildings, facilities, databases etc.
2. *Stored-value transactions*. In stored-value transactions a smart card can be used as an electronic purse (i.e. payment method) to, for example, effect the payment in a public telephone. These payphone cards are the major application category for the stored-

value cards. The more sophisticated smart cards can be recharged with value, while other types of cards are discarded when the credits are used up. Furthermore, the smart card can be used as a credit/debit bankcard, which allows offline transactions.

3. *Portable records*. Smart cards, as portable records, store information that needs to be independent of a fixed location. An example of a portable record would be a medical card, which stores the medical history of a person.

Apart from the above, smart cards can be used, due to their processing power, as a network computing device, personal computing system, banking card, wireless telephony or mobile communications, toll payment mechanism, Internet access card and healthcare card, just to mention a few of the them. The Singapore government has implemented a system known as electronic road pricing (ERP), which communicates with the cars and charges their smart cards as they pass various points on a road.

As smart cards are self-contained and do not need to depend upon external resources, they are resistant to attack. This makes them usable in applications, which require strong security protection and authentication.

All mentioned applications require sensitive data to be stored in the card, such as, information of the card owner, personal medical history, and cryptographic keys for authentication, etc. The application programs handle the data exchanged and communicated between the smart card readers and the institutions, located at the other end of the smart card infrastructure, such as, payment servers in banks and/or credit card companies who process this data.

Overall smart cards are more popular in Western Europe than in the U.S. and are mostly used in France. Due to the popularity of cheques, credit cards and debit cards in America, American consumers regard smart cards as a redundant payment mechanism. The popularity of smart cards in Western Europe and Asia is due to the widely used public transportation system and public phones in these places. According to Dataquest, a market researcher, the smart card market will grow world-wide to 3.4 billion smart cards

in the year 2001 and 4.7 billion in the year 2002. Furthermore, in the year 2001, North and South America combined should make up approximately 20 percent of the market and the Asian market up to 40 percent of the market [112].

Schlumberger,[9] the leader in card manufacturing, projected the following market forecasts for 2001 and even 2003 as shown in Table 6-1. According to the statistics, consumption of smart cards for the year 2003 is expected at 3,100 million units. The consumption of 2,170 million for the year 2001 is an increase of 21% over 2000 [164].

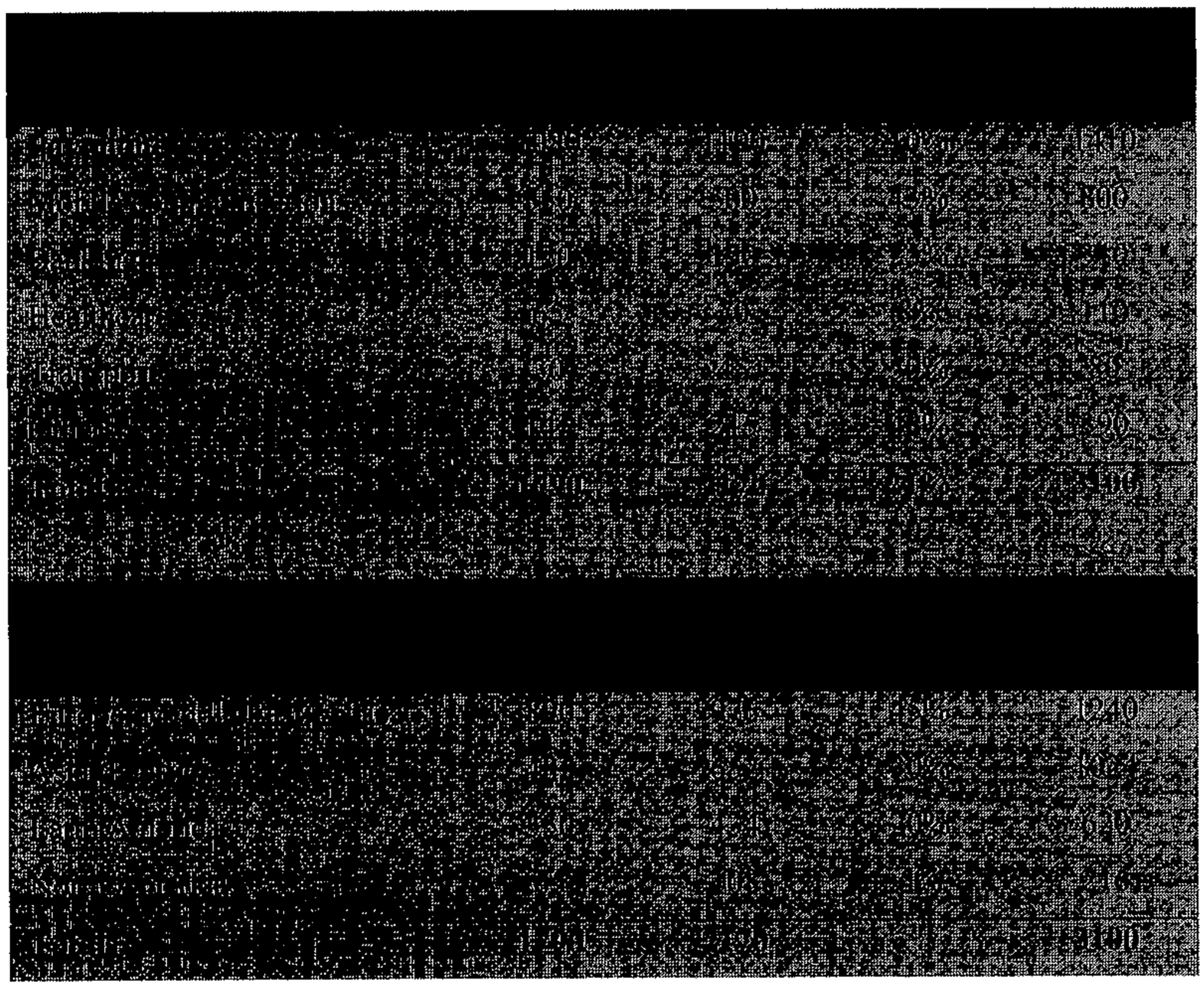


Table 6-1 Projected Growth of Smart Cards (Source: The smart card market in 2001 [164])

Smart cards will be used more and more in the near future. The greatest use is expected in the areas of mobile phones and the Internet [164]. As seen from the above statistics by Schlumberger even the U.S. market, which did not contribute a great portion to the sales of smart cards, promises a major increase in smart card sales. Simon Ormerod, Managing

[9] For more information see the home page at URL: http://www.slb.com/smartcards/

Director of Gilles Leroux says: "The U.S is now opening up to smart cards. Cellular phones with GSM are experiencing an exponential rate of growth. In the context of the Internet, the smart card enables data security and prevents payment fraud" [164]. Due to the security measures in place they may become more popular.

6.6.2 Physical Structure of a Smart Card

The physical structure of a smart card, as displayed in Figure 6-7, is specified by the International Standards Organization (ISO). It is made up of three main elements:

1) The plastic card, holding the same size as of a credit card, with dimensions of 85.60mm x 53.98mm x 0.80mm,
2) A printed circuit, and
3) An integrated circuit (IC) chip.

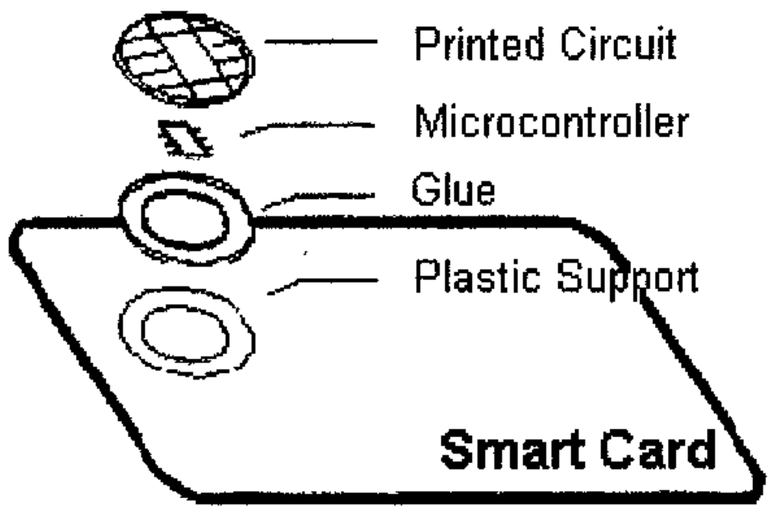


Figure 6-7 Physical structure of a smart card (Source: [15])

The integrated circuit chip performs the functions of a microprocessor. The printed circuit overlays the circuit chip and protects the circuit chip from mechanical stress and static electricity. Communication is established, by transferring information and/or applications stored on the circuit chip when needed, through an electronic module that interconnects with a terminal or card reader [106]. The integrated circuit chip, which makes the plastic card "smart", consists of:

- A microprocessor,
- Read Only Memory (ROM), or sometimes called operating system,
- Non-static Random Access Memory (RAM) or working memory, and

- Electrically Erasable Programmable Read Only Memory (EEPROM) or user memory.

The **microprocessor** is what distinguishes a smart card from a normal memory card. A memory card does not hold an embedded chip microprocessor within the card. The microprocessor is handling all the processing capabilities, controls the three memories (ROM, RAM and EEPROM) and allows information to be stored, processed and accessed online or offline. The **ROM**, storing the smart cards operating system, is integrated at the time of manufacturing and retains its state when the power supply is disconnected. It contains all the operations that need to be executed by the central processing unit (CPU). As the name already indicates, the **RAM** is used by the CPU for temporary storage of information during the "working hours" of a smart card. During power failure all the information stored in this memory is lost. Due to the **EEPROM** the smart card became a re-programmable device. Information stored on the memory cells can be changed, updated or even added electrically. When the chip is manufactured, this memory does not hold any information, but all data is related to a cardholder and application is electrically written during the life of the card. It stores the secret keys as well as personal data, such as, passwords belonging to the cardholder. The EEPROM is divided into four memory areas and will be listed in descending order with respect to the security level [56]:

1. The *free reading area*, or also called open area, stores information that can be read, but not altered without any special authorisation. This area can only be written during the personalisation phase (see below).
2. The *working area* or application memory of the EEPROM is more secure and can only be accessed by authorised persons, i.e. under the microprocessor's control. To avoid unauthorised read, write and erase operations to the data in this area, the card issuer's keys (PIK) is used for protection. Furthermore, the data throughout the card's life cycle is managed here.
3. The *secret area* is strictly confidential and may be written only once. Only the microprocessor can read this area and any access from external resources to this area is not possible. Not even the cardholder can access this area of the smart card.

A smart card communicates with the outside world through the **input/output (I/O) interface**. This interface makes the distinction between "contact" and "contactless" chip cards. The daily operations of a card, such as, reading, writing, searching or erasing protected and/or unprotected data stored on the memory area, are performed by the **operating system**, which is found inside every smart card. The operating system is the key for securing and protecting any data stored on the smart card and therefore, manages resources, such as, the memory, the I/Os and the security.

6.6.3 How does the Smart Card work?

A user needs to access his bank account on the Internet. This access will however only be granted to him after the online bank knows for sure that he has the proper access rights. When a user inserts his card into the smart card reader he needs to "present" a PIN before confidential data can be accessed. The PIN and other passwords are stored in the secret area of the EEPROM and are read and verified by the smart card reader. All the access conditions for every operation (e.g. read, write, delete, search etc.) on every field in the smart card that the user can perform, are stored in the ROM. [100]. To put it differently, complete operations are built into the smart card. The microprocessor is handling all the processing capabilities of a smart card by accessing the operating system and the instructions stored in the ROM. Therefore, the microprocessor will determine whether or not a user is able to perform a certain operation or access a certain program. The CPU controls the input and output through the smart card reader.

When used for payment on the Internet, a user needs in addition to a smart card a smart card reader, a PC and a web browser. In this way he can authenticate himself to a web server. No necessary identification information, for example a key, is needed, as all the data is stored on the card when issued to the cardholder. Payment is done by inserting the card into the reader and having the amount decremented from the card.

Using the smart card as an electronic cash payment model, no transaction processing is required and no additional transaction costs are incurred. The customer sends the cash to the retailer and the retailer sends the goods to the customer.

6.6.4 Logical File Structure and Access Controls

Information in the memory of a smart card is stored using a logical directory and file structure. In terms of data storage, a smart card can be viewed as a disk drive where files are organised in a *hierarchical form* through directories (much like the MS DOS or UNIX file structure). Each directory can be accessed independently under the control of the smart card's operating system and its CPU. This allows both files and directories to have their own access and security levels.

The file system consists of a master file (like a root directory), a dedicated file (like a folder) and an elementary file (like a normal file). The files may store information, such as, owner's surname, address etc. Prior to performing any operations, the file, which stores the data, must be selected. The header of the file indicates the access conditions and current status. Access to any data in these files depends on whether those conditions can be fulfilled and/or whether a person is able to present the PIN numbers correctly.

Five access level conditions for a file can be defined [15]:

- *Always (ALW)*: The file can be accessed without any restriction.
- *Card holder verification 1 (CHV1)*: The file is only accessible when a valid CHV1 value is presented.
- *Card holder verification 2 (CHV2)*: The file is only accessible when a valid CHV2 value is presented.
- Administrative (ADM): The administrative authority determines this access level.
- *Never (NEV)*: Access to the file is forbidden.

6.6.5 Lifecycle of a Smart Card

The lifecycle of a smart card consists of the following phases: fabrication phase, manufacturing and pre-personalisation phase, personalisation, utilisation and invalidation phase. Security measures are considered as early as the first phase of a smart card's life. Many controls and measures are implemented to ensure that no entity or person can obtain knowledge of the design of the chip or the initialisation and personalisation data.

During the **fabrication phase** the circuit chip is created and tested. A fabrication key (KF), which protects the circuit chip phase from fraudulent up and till the end of the pre-personalisation phase, is added to the chip. The KF of each chip is a unique security key, derived from a master manufacturer key and can be accessed only by authorised persons. The chip is then ready for delivery to the card manufacturer.

During **manufacturing** or the **pre-personalisation phase**, the integrated circuit chip, after successful testing, is mounted to an electronic module. This chip-embedded module is then glued to a plastic card, which normally has the logo of the application provider printed on it. The company that performs the embedding function does not have access to the secret cryptographic keys with which the chip is protected, and therefore, cannot tamper with the contents of the chip. Finally, the card manufacturer will test whether a connection between the chip and the printed circuit (i.e. electronic modules) is established in order to test the unit as a whole.

For secure delivery of the card to the card issuer, the personalisation key (KP) replaces the fabrication key. After that, a personalisation lock will be written to prevent further modification of the personalisation key. In addition, physical memory access instructions will be disabled [15]. From now onwards, access to the card can only be done by using logical memory addressing. This preserves the system and fabrication areas being accessed or modified.

During the **personalisation phase**, as the name already indicates, the card is electronically personalised and customised by the card issuer for a specific cardholder and/or application, based on certain requirements. The card issuer completes the creation of the logical data structure. The cardholder's personal and non-personal data, the cardholder's code (PIN), the issuer keys and the smart card secret keys will be written to the memory to be subsequently stored in the smart card. Data files contents and application data is stored in the working area of the EEPROM memory. At the end an utilisation lock VUTIL will be written to indicate that the card is in the utilisation phase.

During the **utilisation phase** the cardholder can use the card. Application data and logical file access controls are activated. The keys specified in the personalisation phase and the security policies set out by the application, will limit information or memory access.

The card has reached the end of its lifecycle or the **invalidation phase** in one of the following instances:

1. The user has entered the incorrect PIN and unblocking PIN too many times (the number of times depends on the system).
2. The normal lifecycle of the card has come around.
3. The invalidation lock is set by the application.

Once the card enters the invalidation phase only the read instructions are active and any writing and updating will be disabled.

In conclusion it can be said that security is offered through the two security keys: the fabrication key (KF) and the personalisation key (KP). These keys are kept secret and are not revealed to others. During the personalisation, utilisation and invalidation phase they are not accessible anymore.

6.6.6 Attacks on a Smart Card

The smart card could become the target for attackers for a few reasons. It is a tool used to store valuable personal information, private keys, account numbers and PINs, and to

provide cryptographic functions, which provide encryption and decryption of data for the card. The access control inside the smart card, is another attractive attack place for attackers. In order to avoid these attacks smart cards must be a security module themselves. They must have built-in security mechanisms to prevent any logical and/or physical attacks, for example, preventing a person from using a stolen card [6].

The attacks on smart card can be separated into:

1. **Logical attacks**. As the electrical charges of an EEPROM are very small, a write operation can be affected by under and over-voltages and temperatures, which means, information can be trapped by raising or dropping the supplied voltage to the microcontroller. This is very dangerous, as all the key material of a smart card is stored in the EEPROM. For example, a short voltage drop can release the security lock.
2. **Physical attacks**. These attacks can only be performed if the circuit chip is removed from the plastic card, using, for example, a sharp knife. In this way the chip can be examined and attacked directly. Other physical attacks include, erasing the security lock bit by focusing UV light on the EPROM, probing the operation of the circuit by using micro-probing needles, or using laser cutter microscopes to explore the chip [15].

6.6.7 Standards for Smart Card Usage

Standards are a key ingredient to the future success of smart cards, and ensure that smart cards and smart card-accepting devices are built to uniform specifications. They therefore, ensure that cards manufactured and issued by different industries or same industries, but in different parts of the world are compatible and can be accepted by any device [112]. Without any uniform specification, smart card interoperability between various industries will be very difficult to achieve.

Standards, which are specific to smart cards, can be separated into two groups, namely: contact and contactless. The *International Organization for Standardization* (ISO) has

developed standards for smart cards for the use by various industries. **ISO 7816** is a global standard that lays out physical characteristics of cards and contacts, transmission protocols, inter-industry commands for interchange, and rules for applications and data elements. **ISO 10536** specifies similar characteristics for contactless cards [106].

For smart cards to act as a computing platform for various applications an **application programming interface (API)** is needed. The API, which is critical for smart cards to carry out diverse functions, can be incorporated into the smart cards processors. Application standards include:

- Electronic purse standards, such a Mondex
- Payment standards, such as, Secure Electronic Transaction (SET)

Standards are continually changing, as further developments of the technology and further applications occur. It is important that innovation within the industry is not constrained by the application of standards, which have become inappropriate.

6.6.8 Smart Card Advantages

The major benefits for smart card users can be categorised as convenience, economic benefits, security, customisation and multi-functionality.

a) Convenience

Smart cards are as small as credit cards and can be easily carried in a pocket or wallet, providing users with mobility and data portability, i.e. direct access to cash or services. They will combine paper, plastic and magnetic cards used for different *identification purposes* into one card, which can access multiple services, networks and the Internet. The chip therefore, reduces the number of cards, making one card the access key to many accounts. Health care cards, for example, reduce document processing costs by allowing immediate access to personalised patient information stored in smart cards [106], which is vital for emergency cases. Smart cards are supported by many industries, real and virtual stores accept them and they offer *standardised user interfaces*.

b) Economic Benefits

Smart cards reduce the transaction costs by eliminating paper and paper handling costs, i.e. providing a *paperless environment*. Using smart cards, redundant time-consuming forms do not need to be completed when doing payment over the network. Costs associated with credit cards are also reduced by smart cards, because they store the information directly on the card and not at a central location.

c) Security

The smart card will be used to carry a lot of sensitive and critical data, depending on the application for which the smart card is used (as discussed above). Therefore, there are many arguments and issues about whether or not the smart card is secure and safe enough to store that information.

The security for the smart card is provided, by ensuring the following security services [84, page 14]:

- Identification and authentication of the user, such as, biometric authentication
- Cryptographic applications, such as, digital signatures and encryption
- PINs are stored for several applications on a single smart card
- Secure storage of data on the smart cards
- Loading and cancelling of units of value for electronic payments

d) Customisation

A smart card is a personal and local application and security anchor, containing all the data needed to personalise networking, Web connection, payments and other applications [106]. They carry personal account information for electronic appliances or even phone numbers that can be accessed by a mouse click.

e) Multifunctionality

Due to the processing power of smart cards they can be used for multiple functions and/or applications. This will of course reduce the overall number of smart cards in the

consumer's wallet. Using smart cards, payment and other applications can be personalised.

6.5.9 Smart Card Disadvantages

Apart form all the advantages the disadvantages are as follows:

- International standards for the smart card procedures and the smart card itself are both still evolving.
- Start-up costs, such as, capital investment and the cost of the smart card itself are not very cost-effective.
- A vast amount of information and possible cash is stored on the smart card. If the card is lost or stolen, there is no way to recover the information or the money. This causes a true potential for fraud.
- Risk of logical attacks, such as, vulnerability to static electricity, magnetic fields, temperature and light. For example, the secret key information of a smart card is stored on the EEPROM, which can be affected by unusual voltages and temperatures. Meaning, information can be trapped by raising or dropping the supplied voltage flowing to the microcontroller.
- Risk of physical attacks, for example, when the chip is attacked directly, viruses and computer hackers.

6.6.10 Mondex as a Smart Card Payment System

Mondex International as the world leader in smart card payment systems, licenses its right to local Mondex originators in each country in order to enable them to create electronic cash units serving as a given nation's currency [106].

The Mondex payment system is a transferable, offline, non-anonymous [123] electronic payment system handling both large and small transactions. The Mondex *smart card* is an electronic wallet that can store electronic cash in up to five different currencies [123] and is used to spent electronic cash over the Internet paying for goods and services in the

same way as cash but with some key benefits over traditional cash. This provides the portability and network independence of physical coins. Using this system, a consumer can browse any online service that accepts Mondex.

Mondex electronic cash is digitally stored on a re-loadable and highly secure computer chip. The chip is embedded in a plastic card that looks and feels similar to a debit or credit card. Though Mondex looks like any other plastic card, it acts similar to cash, due to *chip-to-chip* transactions.

Mondex cards are read at the time of the transaction and verified either through telephone lines, on site through Mondex wallets, which allow transfers between cards, or via the Internet by inserting the card into a standard smart card reader connected to a PC. Inserting the card into a balance reader can check the current balance on the card.

6.6.10.1 How does the Mondex system work?

Mondex value flows directly from one Mondex chip to another Mondex chip. No third-party intermediary clears or processes transactions. Only the holders of the two Mondex chips are involved.

A user opens an account in order to receive the smart card. The smart card is then topped-up with downloaded tokens. In order to purchase items over the Internet, a consumer inserts his Mondex card into the smart card reader attached to his personal computer. Placing the Mondex card in a Mondex terminal (reader) starts the transaction process, as displayed in Figure 6-8:

1. The customer's card is validated by the merchant's chip. Similarly, the merchant's card is validated by the customer's chip, in order to assure that both parties are authorised to make the transaction.
2. The merchant's card requests payment and transmits a digital signature with the payment request.

3. The customer's card checks the digital signature and, if satisfied, sends acknowledgement, again with a digital signature, to the merchant.
4. Once the customer confirms that another valid Mondex device is present on the other end of the transaction, the customer's card transfers value directly to the Internet merchant's Mondex chip. Offline consumers pay for items by swiping the cards through specially designed kiosks.
5. The merchant's terminal checks the customer's digital signature for authenticity. If the customer's signature is validated, the merchant sends his signature again to the customer.
6. The transaction amount (electronic cash) is only transferred to the merchant once it is deducted from the customer's card and once the goods are delivered.

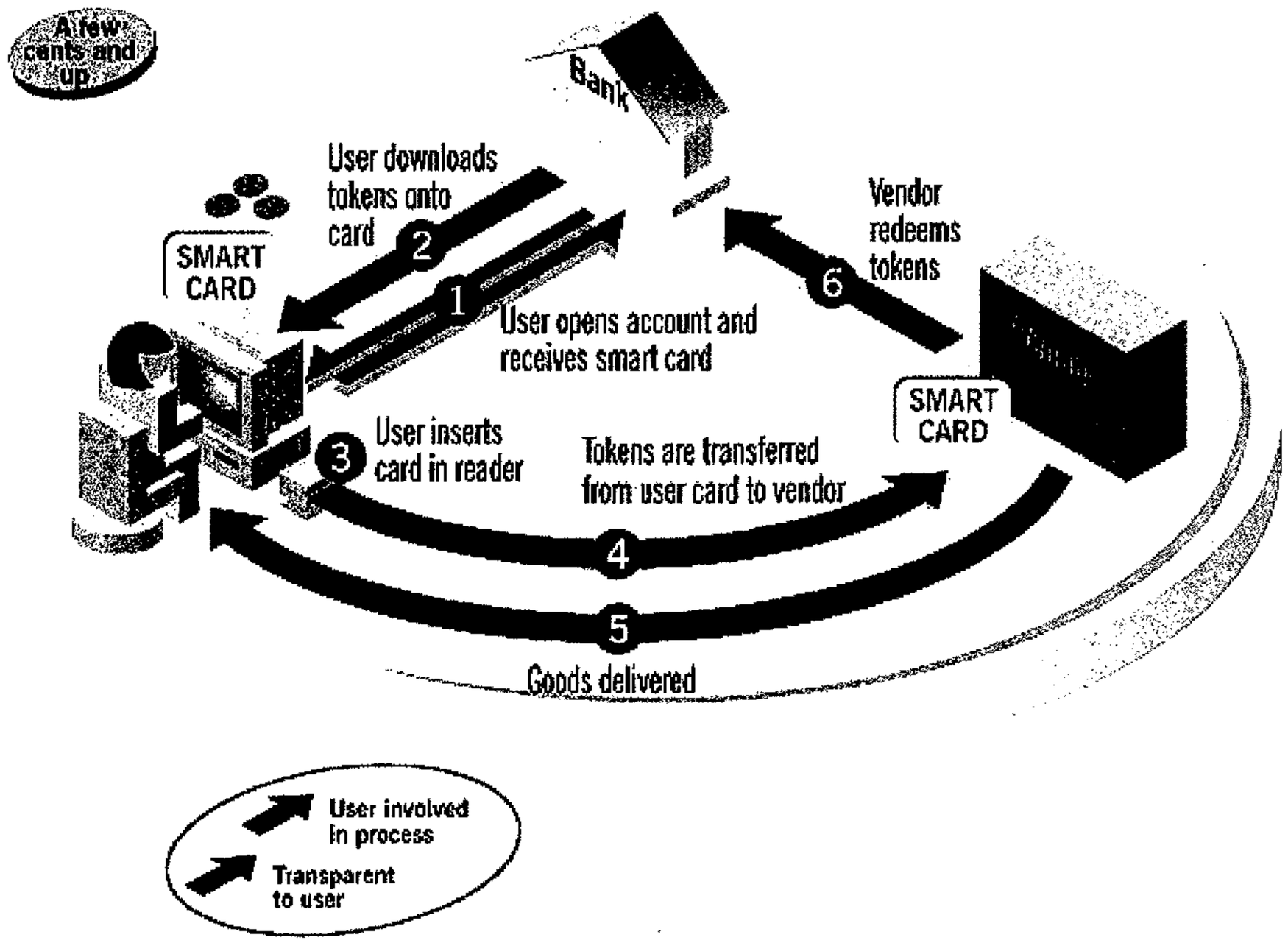


Figure 6-8 Payment transaction over the Internet using a Mondex card (Source: [136])

In addition to a regular transaction, a consumer (who is a cardholder) can also make a payment by inserting his Mondex card into the merchant's Mondex terminal or into

another individual's electronic purse. Furthermore, two cardholders can transfer electronic cash among themselves over a telephone line, without an authorising authority (such as, the bank) being involved in the transaction.

6.6.10.2 Advantages and Disadvantages of the Mondex system

The advantages of the Mondex payment system are:

- Mondex electronic cash will provide a payment alternative to credit cards, allowing purchasing over the Internet.
- A cash/pursue model. Electronic purses are a special variant of the token-based system, as they require special hardware of the smart card variety.
- Pre-paid value storage.
- Mondex allows the handling of smaller transactions, even under a dollar. As already mentioned these kinds of transactions are not suitable for credit or debit systems, as they are too expensive to handle.
- Mondex handles multiple currencies and multiple applications.
- Cash is transferred from a Mondex card to a Mondex offline merchant terminal within a few seconds, making card-to-card transfer possible.
- There's no authorisation and no central clearing of transactions, which means no dedicated phone line is needed.
- Due to the "chip-to-chip" feature consumers can conduct local or remote transactions with Internet merchants and their banks, simply and quickly. Merchants can immediately receive cash value at the time of the transaction, leaving the merchant's payment guaranteed.
- The customers can "pay as they go" and even transfer cash between their cards over a telephone line, decreasing their checkout time at the register.
- The merchant's cash handling expenses are reduced as the staff spent less time in the handling of cash and preparing bulky cash deposits, which then have to be taken to the bank.

The disadvantages of the Mondex payment system are:

- The Mondex bank knows too much about the transaction details.
- A smart card balance reader is required if customers want to check the balance of their card at any time.
- The Mondex card carries real cash, which can be a risk in the case of theft.

The biggest advantage of the Mondex system is the ability to use it in real world [60] as it can be used to pay for goods and services in the same way as cash. In this way the Mondex system provides the portability and network independence of physical coins.

6.7 Internet Credit Card Payments

Credit cards and charge cards, collectively termed payment cards, will operate much in the same way as they currently do, with the exception that a different medium is involved in transmitting the customer's transaction information to the merchant. The customers will use the web browser to fill in the order form and the web server will process the form and forward the authorisation request to the bank network. Furthermore, in an electronic version of a credit card payment a new role, apart from the traditional cardholder, issuer, merchant and acquirer, is involved: the payment gateway.[10]

The steps in the electronic credit card payments are the following:

1) The customers use the web browser to fill in the order form. (The web server will process the form and forward the authorisation request to the bank network.)
2) The merchant sends an invoice to the customer.
3) The customer sends a payment instruction to the merchant.

[10] The payment gateway is a system (operated by a designated third party) that handles the financial request from the merchant and interacts with the issuer on the merchant's behalf. In CyberCash [129] the payment gateway is represented by the CyberCash server.

4) Once the merchant receives payment from the customer through the Web page form, he will pass the customer payment card information to the acquirer (merchant's bank).
5) The acquirer will use the financial networks to authorise the payment and returns an authorisation response to the merchant. Furthermore, he will credit the value of all the sales slips to the merchant's account.

There are established methods, like Netscape's SSL based on RSA's public key encryption and the SET protocol system, for ensuring secure transmission of the client's credit card number to the vendor. Companies employing credit-based payment methods on the Web should support the SET protocol system. This protocol system safely communicates or presents credit card numbers during credit card transactions over the Internet.

To make card payments possible on the net, virtual credit cards are needed to replace "real" credit cards. These virtual cards are known as so-called certificates. These certificates must be presented during each Internet payment procedure. They guarantee for the authenticity of all participants involved in a transaction process. Furthermore, in order to protect the transmitted credit card number during data communication, it should be encrypted. A third party is used to decrypt the credit card number. These third party systems are available from CyberCash and First Virtual.

In a **closed loop** payment processing system, banks and other financial institutions serve as a broker between card users and merchants. **Open loop** systems involve a third party such as, a local bank, credit union or some other clearinghouse operation.

6.7.1 Strengths and Weaknesses of paying by Credit Card

To pay by credit card on the Internet offers a high degree of security and the already existing, high-quality infrastructure maintained by the credit card institutions. However, credit cards are not suited for payments of smaller amounts, due to the relatively high

transaction costs. Due to the lack of the personal signature required in the case of conventional credit card payment, there is a danger of misuse, although the risk here is considerably less than in the case of payment by telephone, or in a restaurant, for that matter.

Unlike cash transactions that are anonymous, credit card transactions link a name to the account. Therefore, the customer will not be able to maintain the *anonymity* of a cash transaction. They also run the risk of having their name added to a number of mailing lists, which implies lack of privacy.

The *durability* of the transaction is an issue for credit card transactions over the Internet. It is possible that a transaction may be interrupted in the middle of the process, leaving one party unsure whether a transaction did or did not occur. The key to ensuring that transactions are durable is by remaining faithful to basic contract law.

6.7.2 The SET Protocol

The SET protocol [154] was developed by the two major credit card institutions, **Mastercard/Eurocard** and **Visa**, who have jointly decided on the first *global security standard* for the secure transmission of credit card data via the Internet. SET is an *encryption protocol* that performs authentication of both parties to a transaction, using digital signatures, digital certificates and public key cryptography.

Under the SET protocol, both the buyer and the seller obtain a digital certificate from a trusted certification authority to validate each other and to establish trust in the electronic payments process. The cardholder generates a private and public key in his/her own computer. The private key is kept secret by the cardholder, whereas the public key is communicated to the bank, which will then issue a certificate (signed by the bank) to the cardholder. The digital certificate is a digital analogue of a credit card but does not include the account number and expiry date. It binds the credit card number of the

cardholder and his public key. Each certificate rests in a wallet at the relevant machine and the issuing card company can only decrypt the credit card details contained within it.

The SET certificate allows merchants to display the SET logo on their products. In fact, a web site is only SET certified if the homepage displays a logo indicating that it is SET certified. Upon purchase, the merchant presents to the customer two digital certificates. One certificate proves that the merchant supports the SET specification, while the other certificate identifies the payment gateway [48].

In order to leave the "traditional" banking network infrastructure unchanged, a payment gateway is used to act as interface between the Internet and existing financial networks. Therefore, the payment gateway will convert the electronic requests coming from the Internet into their traditional format [31] for processing by the cardholder's banks. Furthermore, the verification of certificates and digital signatures is done by the payment gateway and not at the cardholder's bank.

6.7.2.1 Blinding in the SET Protocol

Using the SET Protocol the credit card numbers in the certificate are blinded. In this way the credit card numbers are protected from credit card fraud, as they are never sent "unprotected" over the Internet. The certificate stores an *unique cardholder identity* [31], instead of the credit card number, as the cardholder's account information. This identity is then used by the payment gateway to identify the cardholder account.

6.7.2.2 How does the SET transaction work?

With the SET process, traditional card-based payments at the point-of-sale (POS) are relocated into the Internet. The SET-based transaction process, as displayed in Figure 6-9, functions as follows:

1. A SET-compliant cardholder visits a cyber-storefront via a browser. After selecting the items to be purchased, the customer (online shopper) fills out a payment request,

and selects from an on-screen electronic wallet (SET wallet) the credit card he wants to use. The customer transmits the payment request to the payment gateway (or merchant's web server), along with his/her digital certificate.

2. At the payment gateway the information is encrypted under the payment gateway's public key and sent to the merchant.
3. The merchant uses a so-called virtual POS system, which is basically a carbon copy of POS terminals found at the merchant store's cash point. The merchant generates a request-for-payment authorisation from the cardholder's financial institution [117]. His digital signature, transaction identifier and payment instructions are included in the encrypted request and forwarded to a payment card-processing centre or payment gateway of the acquirer [48], where it is decrypted, processed and verified.
4. After the SET transaction is verified the payment card-processing centre converts the SET authorisation request into the format used by financial networks and then forwards it for approval to the cardholder's bank (issuer) for authorisation.
5. The issuing bank returns an approval or denial response to the payment gateway in response to the authorisation request. The payment gateway will send this response (authorisation or failure) to the merchant.
6. If the bank approves the authorisation, the payment gateway sends a notification in the form of a digitally signed and encrypted message to the merchant [48], which can be claimed later from the merchant's bank for deposit.
7. Once the merchant has received the payment gateway's digital signature he will ship the goods to the cardholder [44], knowing that the customer transaction has been approved.
8. The merchant will request settlement from the issuer, via the payment gateway via the acquirer [129].

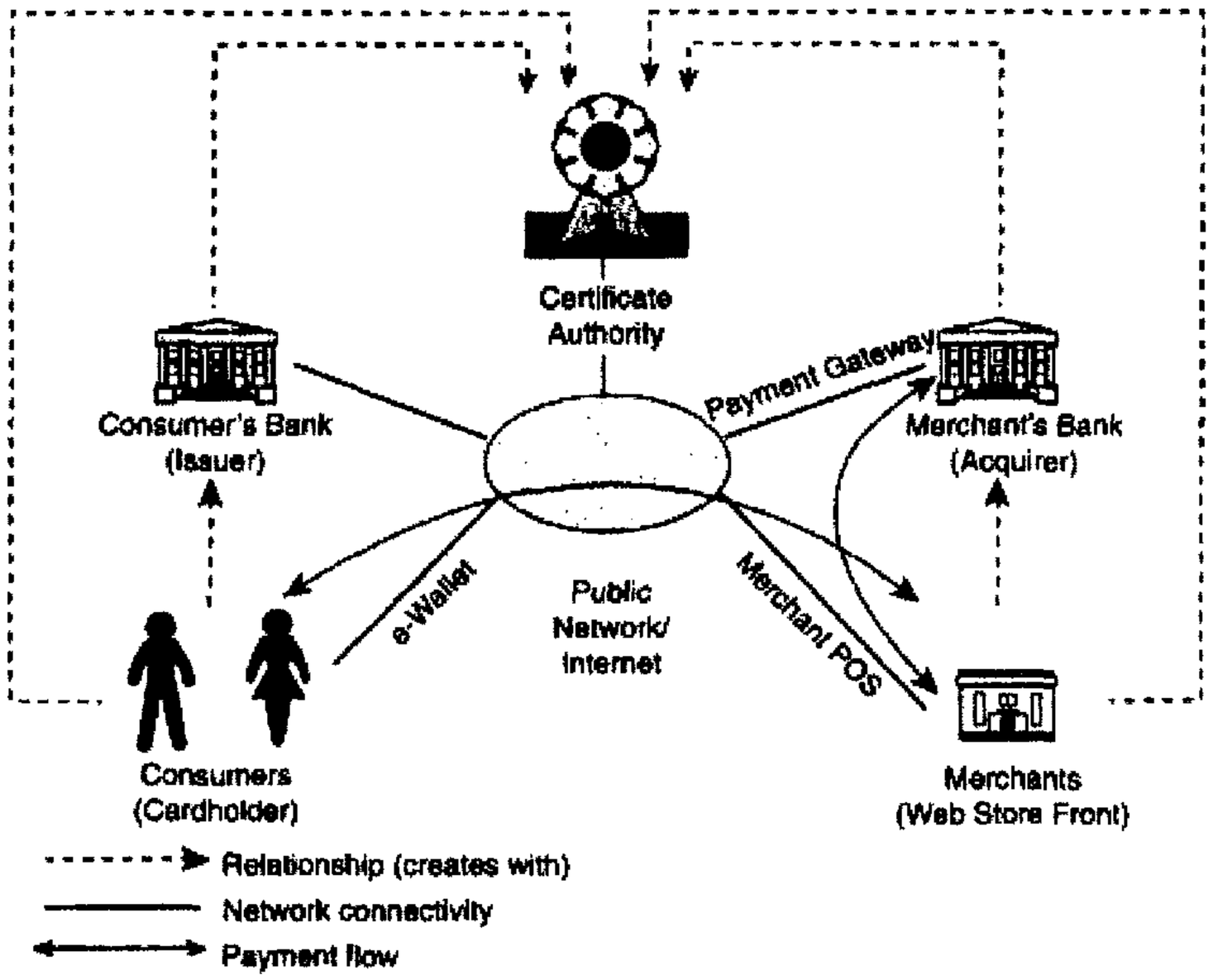


Figure 6-9 Phases of a SET-protected credit card payment transaction (Source: [48])

Logically speaking, this virtual system is no different than the POS terminals that are found today next to almost every cash register. The Internet helps extend the merchant's card scanner all the way to the customer's PC, where it is then depicted in the form of a "virtual wallet".

6.7.2.3 Advantages and Disadvantages of the SET Protocol

The two major advantages offered to the consumers by SET are **security** and **comfort**. SET meets all security requirements of confidentiality, integrity, availability, authentication, and non-repudiation.

Other advantages of the SET protocol include:

- Guaranteed payment for the merchant.
- As a result of the encryption used in the SET process, it is no longer possible for unauthorised persons to gain access to a credit card number or to use cards illegally.

- Merchant does not have to access to the buyer's credit card number.
- Compatibility with existing credit card contracts.
- World-wide acceptance of credit cards could increase the acceptance level of the protocol.
- Ease-of-Use. Each transaction participant receives an electronic wallet, which handles the payment process for him or her automatically. Payments can now be made with the click of a mouse.

The disadvantages include for both the consumer and the merchant include:

- Extra software is needed. A SET purchase requires encrypted transactions and consumers need digital certificates. Both merchants and customers will need to install the special wallet software.
- The e-wallet is subject to theft, holding all the credit card numbers, digital certificates and personal information of the e-wallet owner.
- Card issuers must invest considerable sums to have public key pairs and certificates issued to their cardholders. The benefits to the SET card issuers are sometimes not clear [8].
- Each successful attack upon a CA means the compromise of the private key of that CA.
- It is not clear that SET will generate significant new credit card volume, as opposed to merely displacing mail and telephone orders.
- There exists no smart card support for signatures.
- Not suitable for micropayments, due to vast amount of messages (including, digital signatures, encryption and decryption operations etc.) between customer and merchant.
- If SET would be widely adopted, the number of certificates would increase, making the process of certificate redistribution time consuming and costly [8].

6.7.2.4 Difference between SET and SSL

Secure Sockets Layer (SSL) and certificates can be used to improve the security of message contents and to guarantee the identity of their senders. SSL uses quite sophisticated cryptographic techniques to ensure the link between the customer and the merchant and for transmitting credit card numbers on the Internet. SET uses digital certificates to verify the identities of both the consumer and the merchant, focussing on ensuring confidentiality and authentication

The current competition between SSL and SET comes down to the allocation of risk. SET makes the buyer responsible for proving his credentials whereas, with SSL, it is up to the seller to check the buyers' ability to pay. Without SET protection, sellers are faced with users denying they have made particular transactions and cannot prove that they did so [67]. Using SET, credit card companies will absorb the cost of any fraud, whereas for SSL the merchants must absorb the cost of the fraud.

6.7.3 CyberCash as a Credit Card Payment System

As already mentioned under the CyberCoin system, **CyberCash Inc.** [120] provides features for all types of Internet payments including cash payment systems and credit card payment systems. In this section the credit card based payment mechanism part is discussed. The CyberCash payment system, introduced in **April 1995** [92], acts as a *gateway* between the Internet merchant and the banking networks of major credit card brands [123], authorising the payments directly from the customer's bank account or credit card. CyberCash's Internet payments business was acquired this year by VeriSign [120].

A CyberCash consumer must first register with CyberCash, after which he/she is given (or can download) the CyberCash "electronic wallet" software, to make purchases [60]. Like a physical wallet the software wallet can be used by the consumer to register several credit cards. The electronic wallet software contains an encrypted copy of the consumer's

credit or debit card information. Another software package provides similar services to the merchant.

6.7.3.1 How does the CyberCash system work?

CyberCash consumers generate a public-private-key pair when they register their credit card or bank account with the wallet software. The public key is sent to CyberCash payment server, where it is maintained and mapped to the users unique CyberCash ID. The ID is used to unlock the wallet, whereas the data and secret keys are stored in encrypted form. Merchants also hold a public-private-key pair. CyberCash's public key is build into the consumer's wallet and merchant's software. Only the CyberCash server knows the consumer's and the merchant's public key. When the consumer and merchant are communicating with each other they rely on the CyberCash server to authenticate all signatures. In this way the merchant does not see the consumer's credit card number, as this information is always encrypted using CyberCash's public key.

After receiving or downloading the electronic wallet, electronic dollars can be send at any web site accepting CyberCash. When a purchase is made, the consumer requests the item desired. The merchant's server returns a signed payment-request message, which describes the purchase and indicates which credit cards the merchant accepts, through the consumer's Web browser. This message causes the wallet software on the consumer's machine to display a window that lets the consumer select the credit card that he wishes to use and to approve the purchase and the amount. The payment request along with the consumer's encrypted credit card number and the public key of the CyberCash server is sent back to the merchant. The merchant then forwards the payment message, along with the merchant's own signed and encrypted description of the transaction through the CyberCash server to the bank for authentication and approval of the purchase. The merchant cannot see the credit card number as the payment request is encrypted and can only be decrypted by the CyberCash server. The CyberCash server decrypts and compares the two messages and their signatures. If they match, the CyberCash server contacts the customer's bank and transfers the funds to the merchant's own account,

submits an authorisation request and returns the charge response to the merchant. The merchant's software confirms the purchase to the consumer's wallet software. Note merchant's deliver the goods encrypted and provide the key only after payment is confirmed. As it can be seen all the communication is done through the CyberCash server using the CyberCash public key. Figure 6-10 shows the CyberCash payment model.

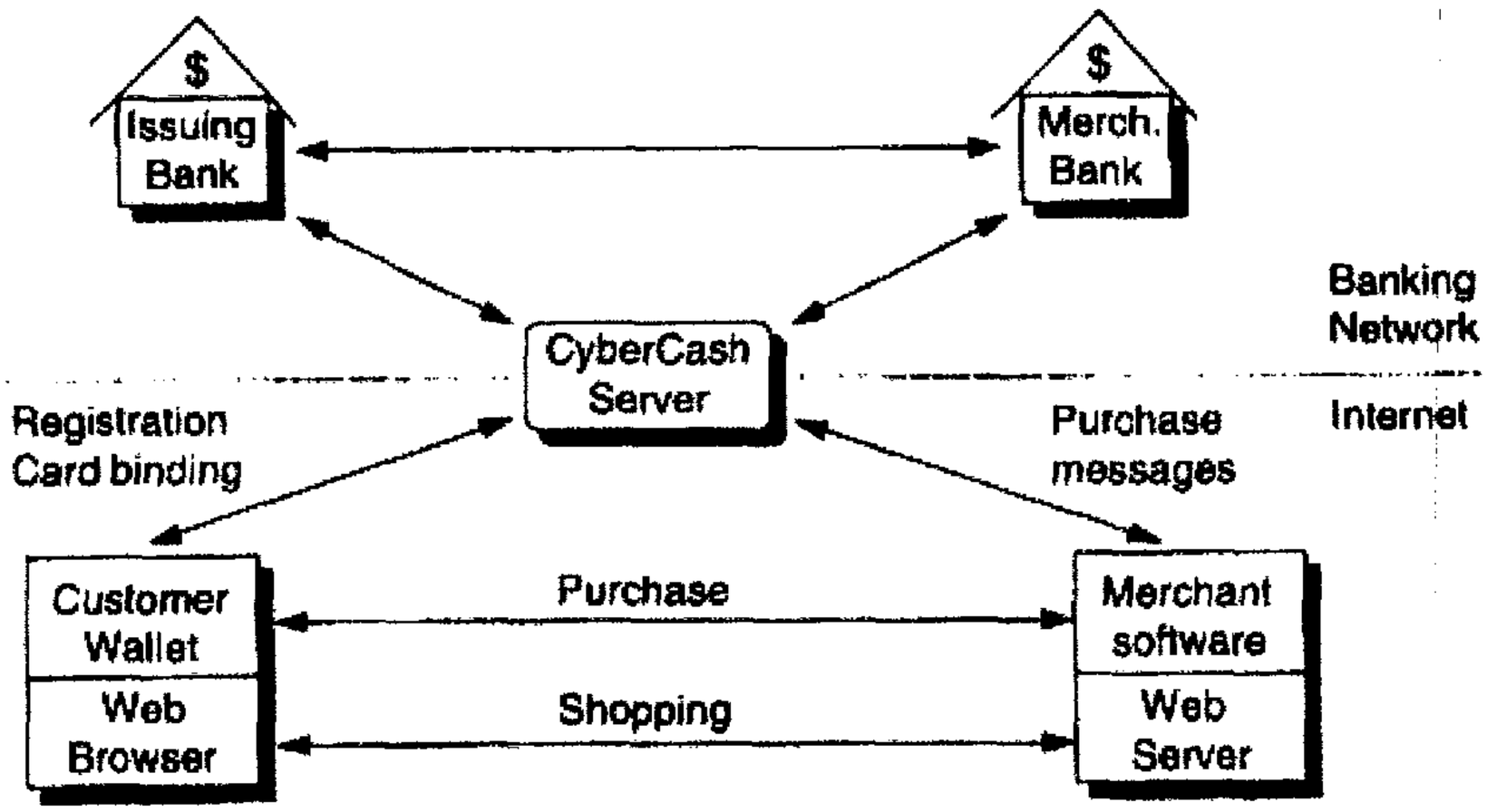


Figure 6-10 Overview of the CyberCash Payment Model (Source: [79])

6.7.3.2 Advantages and Disadvantages of the CyberCash system

The advantages of the CyberCash payment system are:

- Ensures secure credit card presentation payments [92].
- Transaction validation and confirmation is done through the CyberCash server who is a trusted third party.
- The merchants have nothing to loose, as the goods are only shipped after payment is confirmed [159].

The disadvantages of the CyberCash payment system are:

- Only U.S. citizens can bind their bank account to the Wallet software, non-U.S. citizens need a credit card.

- CyberCash Wallet software is required [44].
- Merchants will be charged a transaction fee.

CyberCash has adopted the new SET protocol and is incorporating it into the CyberCash's suite of Internet payment solutions. The transition to SET will provide secure, open standard-based solutions for the merchants, banks and consumers.

6.7.4 VirtualPIN as a Credit Card Payment System

First Virtual (FV) Holdings [132] has implemented an offline e-mail based system, for Internet payment. This credit electronic payment system, called the VirtualPIN, does not require credit card numbers to be transmitted across the Internet and is suited for low to moderately priced information sales. The *goal* of First Virtual was to use only the WWW and e-mail in order to avoid special purpose software and protocols for selling low-value information.

6.7.4.1 How does the VirtualPIN system work?

Consumers and merchants register with First Virtual by phone or e-mail and receive an ID number or PIN in exchange for their traditional credit card numbers. The PIN is used as a pseudonym to identify the consumer during a transaction and refers to his First Virtual account. When consumers want to buy something electronically, they simply supply their PIN, instead of the credit card number to the merchant. Upon receivement of the PIN, the merchant contacts First Virtual for approval, providing them with the details of the sale and the consumer's PIN, to verify that the PIN is valid. First Virtual then confirms with the consumer via e-mail if they are willing to pay for the information. Consumers can reply indicating "Yes", "No", or "Fraud" [129]. "Yes" confirms the transaction. "No" cancels the purchase. "Fraud" is used when a customer has never initiated, such as, transaction. If the transaction is accepted by the consumer, First Virtual converts the PIN to a credit card number and charges the consumer's credit card accordingly to clear the purchase. Subsequently, an e-mail is sent to the merchant

authorising the transaction [34]. After holding the funds for 90 days [79], the company transfers the funds to the merchant by means of an automated clearinghouse. Therefore, the customer gets the product before paying for it and the merchant gets a delayed payment through the automated clearinghouse. Sending the payment approval request by e-mail, while goods are typically delivered over the Web, First Virtual believes that it is hard for an attacker to abuse the system. Figure 6-11 shows the use of the First Virtual payment system in a transaction.

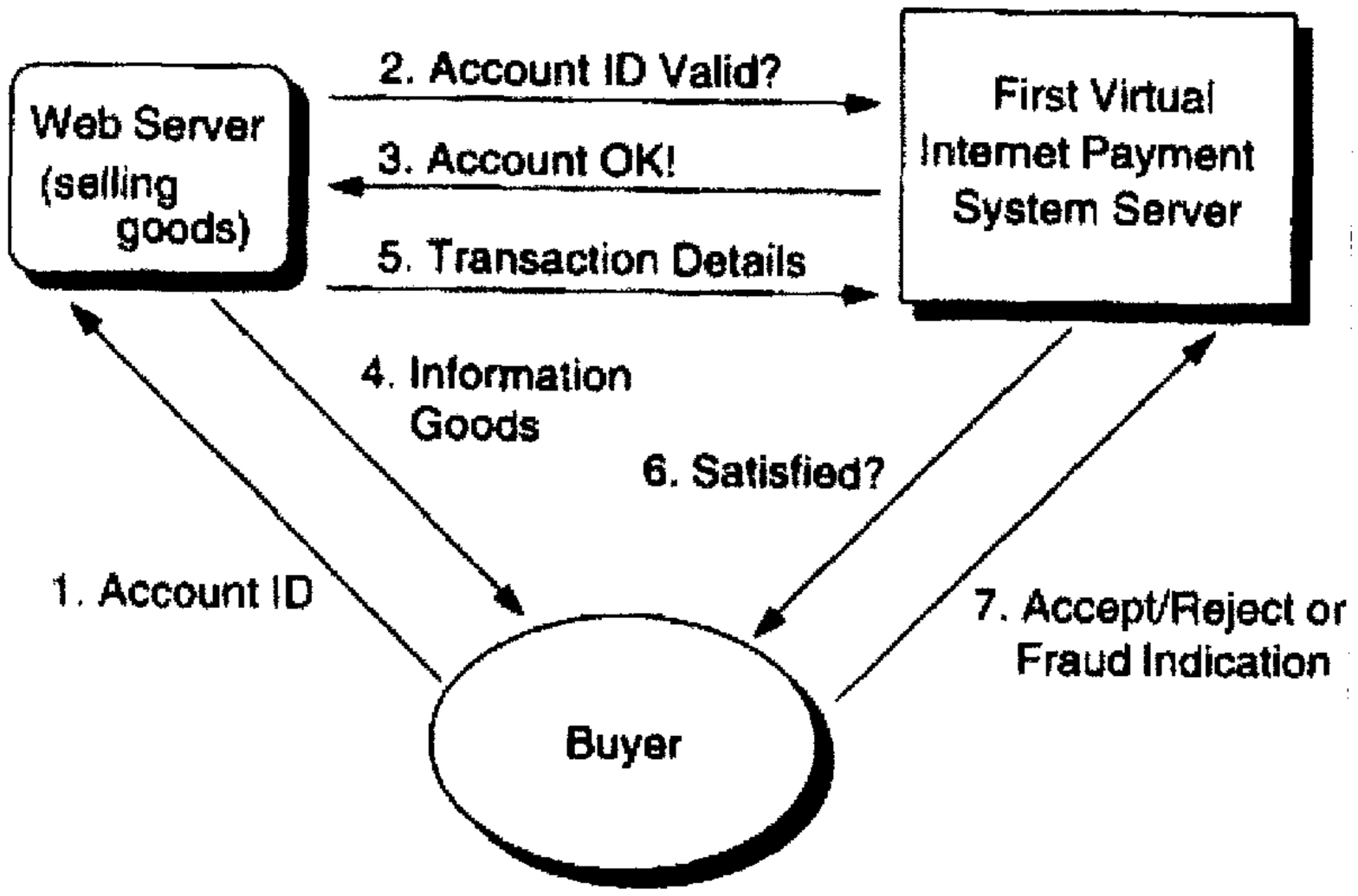


Figure 6-11 Buying with First Virtual (Source: [79])

6.7.4.2 Advantages and Disadvantages of the VirtualPIN system

The advantages of the First Virtual payment model are:

- Ease of use. Neither buyer nor seller needs to install any software in order to use the system.
- Confirmation is provided by the e-mail system, which leads to minimal risk. The card numbers are stored away on a protected computer system and are never passed over the network.

- The cost of sending information electronically "on approval" is negligible, so a merchant has very little to loose if a consumer's answer is "no." However most consumer's are honest and will not systematically order goods and then answer "no" even when they are unsatisfied. But in order to cater for dishonest behaviour, First Virtual will cancel a consumer's account if the pattern of usage suggests abuse.
- By not charging consumers until they are satisfied, the system eliminates the cost of reversing charges for information that was not delivered as a result of network or computer problems.

The disadvantages of the First Virtual payment model are:

- It is very cumbersome to always confirm the sales with the consumers.
- The company relies on the integrity of the Internet's e-mail infrastructure to ensure that a real consumer is answering "yes" or "no". There is no message confidentiality.
- The settlement process is very long and the merchant gets a delayed payment.
- The merchant assumes all risk [57]!

First Virtual Holdings exited the business in **July 1998** [24], [122] and reinvented itself as MessageMedia, Inc [92]. The system was unique in that it did not use encryption. It was based on existing Internet protocols, with the backbone of the system designed around Internet e-mail and the MIME (Multipurpose Internet Mail Extensions) standard [57].

6.8 Customer Accounts

A further type of payment system is invoicing via a customer account that is offered by middlemen/brokers. These are usually online services or so-called electronic marketplaces on the Internet. The intermediary always enters into a contractual relationship with the customer and the merchant. The customer maintains an account with the intermediary for summation of payment amounts, on the basis of which he or she is billed at regular intervals.

The customer's account is well-suited for payments of small amounts. The system administrator can accumulate customer transactions for billing at regular intervals, meaning the customer incurs practically no costs per individual transaction. This, in turn, makes it possible to bill very small amounts. The intermediaries are compensated in the form of a share of sales or unique or regular fees.

6.9 Conclusion

Electronic payment mechanisms are a prerequisite for the materialisation of e-commerce. These payment mechanisms provide a new means of conducting transactions. There are more and more emerging electronic payment technologies attempting to provide secure methods for making payments over communication channels, such as, the Internet. These payment options have been discussed in this chapter – electronic cash, electronic tokens, electronic cheques, electronic wallets, smart cards and electronic credit cards.

Some of the *e-cash players* identified (systems claiming to be "micropayments") among many others are: DigiCash, CyberCoin, NetCash and MilliCent. All electronic cash or token payment models offer anonymity models, except CyberCoin. The degree of anonymity however differs from system to system.

Electronic cheque systems can be viewed as an enhancement and not replacement from the traditional cheque mechanism as they function in a very similar way. The traditional paper cheque is replaced by an electronic document and a digital signature replaces the hand-signature.

Compared to conventional data transmission devices, such as, magnetic-stripe cards, *smart cards* offer enhanced security, convenience and economic benefits. In addition, smart card-based systems are highly configurable to suit individual needs. For smart cards to gain a wider acceptance, interoperable hardware and more applications must

appear to satisfy consumers. As a smart card scheme, Mondex offers the advantage of low value transactions as no third party involved, imposing no transaction costs.

Credit card sales over the Internet are not distinctly different than credit card sales offline. Credit card transactions leave the same paper trail over the Internet as they do at points-of-sale. The same information gathering is possible by governments who want to examine an individual's purchase record. Similarly detailed information about the transaction is available to merchants, financial institutions and credit card companies. Because the transactions of the CyberCash and VirtualPIN system are linked to the customer credit card, the transaction properties are essentially those of the standard credit card purchase. MasterCard and Visa stated that they believe the SET standard will speed the acceptance of commerce on the Internet [136]. SET is a protocol that has secure data transmission as its primary objective. To establish a secure credit card transaction, the payer's credit card number is encrypted using public key cryptography. SET is perhaps the most universal of all electronic payment systems, designed to work with any software or hardware platform.

In order to gain business and customer acceptance of the electronic payment mechanisms and to make them effective, commercial and security requirements must be met. The benefits to be derived from such systems include reduced processing costs, reduced lead times for making payments, increased interoperability, and increased flexibility. The successful electronic payment system will need to incorporate security measures, such as, encryption, digital signatures and authentication. The key is to find a few widely accepted mechanisms, which can be used by most actors.

No matter who develops the best electronic payment system, consumers and businesses alike stand to big benefits. No longer will consumers have to wait for change or stand for in long rows at the automated teller machines for cash, for example. The electronic payment systems will let businesses carry out transactions around the world without transferring bank funds and they will be better able to reach a large population of consumers.

Chapter 7

Traditional Payment Methods versus New Internet "Money"

7.1 Introduction

The biggest difference between the physical market and the electronic marketplace is that some of the components, such as, players, products and processes are electronic, digital, virtual or online.

Various electronic payment systems have been proposed for use in the electronic marketplace, whereas the traditional payment systems are still used for payment outside the network. Despite the technical variations between different paper-based and electronic payments systems for transferring deposit money, the goal of all these systems is essentially the same. The monetary claim of the person making a payment is reduced and the claim of the person receiving the payment is increased.

Whether the electronic payment systems will be as widely accepted as the traditional ones depends, apart from various other factors, to a great extent on the transaction security provided by such payment systems. In this chapter the traditional and electronic payment systems (i.e. cash, smart cards, debit and credit systems) are compared, according to the security techniques offered. Section 7.2 addresses the traditional and electronic cash payment systems, section 7.3 discusses smart cards, and section 7.4 focuses on traditional and electronic debit and credit systems. Apart from this, in section 7.2 – section 7.4, the electronic payment systems are compared according to the following evaluation criteria:

1) **Status and Milestones**. Overview of the main system achievements and to what extent the system is used in practice.

2) **Availability (access)**. The access of a payment mechanism is dependent upon who is allowed to use the payment system.
3) **Convenience**. How convenient it is to use the payment systems, i.e. what are the benefits gained when the system is used? Users want to use a system as easily as taking money out of the wallet and without too much additional effort, such as, the download of additional software.
4) **Security**. Security focuses on three important attributes, such as, anonymity, double spending and the security techniques used. For a payment system to be secure some aspects must be considered. Both, the customer and the merchant need to be identified to ensure that they are authorised parties. For example, it must be possible for the payers' banks to verify that people authorised to use accounts generated payment instructions. Electronic payment information should not be disclosed to unauthorised people and should be difficult to alter. Furthermore, third parties should not be able to monitor any payments made in order to assure confidentiality.
5) **Support of micropayments**. There should exist payment systems that support transaction amounts of less than one cent.
6) **Merchant risks involved**. From the merchant's perspective, the risks are forged or copied payment instruments, insufficient funds in the customer's account, and dishonest or slow financial service providers. From the customer's perspective, risks, such as, stolen payment credentials and passwords, dishonest merchants or financial service providers and disputes over quality of services or goods exist.

The chapter concludes with assigning a score to each electronic payment system and a discussion of the different payment systems according to how applicable they are.

7.2 Comparison of Traditional Cash and Electronic Cash

Real money provides a very simple proof of its *genuineness*: it is physically present. This physical presence of course establishes a great deal of trust as the parties involved in the transaction have direct contact. Coins and notes are produced by means of elaborate

processes involving the integration of watermarks, serial numbers etc. into the money. This is done to eliminate any doubt as to its *authenticity*.

Electronic coins, on the other hand, must demonstrate that they are genuine on the basis of a certain algorithm. Digital cash is made possible by public-key cryptography and digital signatures. The banks sign the money orders using their private key and the customers and merchants verify the signed money orders using the bank's published public key [65]. Customers' withdrawals and deposits are signed using their private keys and the bank uses the customer's published public key to verify the signed withdrawals and deposits.

Traditional cash is the most popular conventional payment instrument and offers a number of attractive payment properties [79]:

- Acceptability,
- Guaranteed payment,
- No transaction charges,
- Multi-currency solutions,
- Privacy, anonymity and untraceability.

Several electronic cash systems have been proposed, satisfying some of those properties. According to Choi [191] an electronic cash system must include the properties of authentication, non-refutability and anonymity.

All electronic cash payment systems are trying to achieve two main requirements: anonymity and micropayments. Electronic cash is collected during payment and is available immediately to either the merchant or the merchant's bank. It offers absolute customer *anonymity*, while at the same time meeting the high security demands placed on digital money. The payee does not know the payer's identity, whereas the issuing bank may or may not keep track of the identity of the recipient of electronic bank notes. The anonymous digital money is the electronic cash provided by DigiCash and NetCash, whereas DigiCash's full anonymity provides far more anonymity than NetCash. The DigiCash solution is substantially more complex than all others, the reason being that this

solution is attempting to provide anonymous payments, and low-cost is only a secondary goal.

Digital cash also presents as many potential risks as it does opportunities. Confidentiality makes it easier for money to be "laundered" through the Net, avoiding the research efforts of law enforcement officials' [65]. In order to prevent this money laundering, government officials might tap digital voice communications and keep track of digital cash transactions. This is of course in conflict with a digital cash system. Another disadvantage of electronic currency is the large database of previous transactions that needs to be maintained in order to detect double spending. In Chaum's approach, every certificate that is deposited is recorded. Apart from this, electronic cash faces the same problem as traditional cash: cash can be stolen. If PC systems crash or if computer hackers enter the e-cash system, the e-cash could be lost forever.

To a large extent, a system's ease of use depends on its transaction processing structure. While CyberCash's CyberCoin asks the user simply to click on an icon, VirtualPIN demands that the user enters and forwards a serial number to the vendor for each purchase [136].

To determine the evaluation requirements provided by electronic cash or electronic token systems, the details of the each electronic cash payment system will be assessed separately.

7.2.1 Evaluation Criteria of the DigiCash eCash System

1. Status & Milestones

Since 1999 eCash Technologies Inc. are offering a secure and *anonymous* cash-like electronic payment system called eCash. The system is available for many Internet-connected computer platforms.

2. Availability (access)

The DigiCash system is available to all consumers and merchants who hold an eCash bank account. Coins are purchased from an online bank and then stored on the consumer's hard drive. It is therefore not necessary for the consumer to go to the bank every time a transaction needs to be made.

3. Convenience

The consumer can spend the digital money at any shop accepting eCash, over any computer network. Any merchant can accept DigiCash without having to undergo a lengthy qualification process. Although the consumer and the merchant do not need any special hardware requirements, consumers need the eCash wallet and they have to deal with the accumulation of spare change.

4. Security

Each eCash coin is a 64-bit encrypted number, with an encoded signature of the issuing bank, making each *coin unique*. This protects the payer's identity and prevents any double spending. In the event of fraud, each coin can be split into its component parts to determine the issuing source of the coin. Double spending is detected via online reference to the central database that keeps tracks of all tokens redeemed. During double spending, the clients give away enough information to detect their identities.

Using *public-key cryptography*, the digital tokens are said to be secured and can be registered and verified by the issuer without revealing to whom it was originally issued.

The DigiCash model has developed the *blinding technology* with the intention to provide full anonymity and untraceability for the customers. The blind signatures allow issuers to digitally sign bank notes without being aware of their serial numbers. The customer chooses the serial number and then blinds it. The coin issuer signs the blinded version and returns it to the customer who then unblinds it. If all parties collide, nobody will know who spent the currency.

The eCash therefore, complies with the "*anonymity*" attribute, when compared to the attributes achieved by the conventional systems and provides the privacy of paper cash. No authentication is needed to spend or receive eCash, and its use leaves no audit trail. Neither the bank nor the merchant can track consumer purchases [159]. Although the current implementation of eCash fully protects the identity of the payer, unless they decide later to prove the payment, it is traceable as regards the payee. The payee is identified as soon as he deposits the coins for validation in order to clear the transaction.

5. Support of micropayments

DigiCash supports micropayments.

6. Merchant risks involved

The merchant is able to detect double spending and receives immediate payment, which of course reduces the risk of unpaid transaction. The customer is at limited risk with the tokens in the electronic wallet, whereas the merchant has no risk because of online validation and prepaid accounts.

7.2.2 Evaluation Criteria of the CyberCash CyberCoin System

1. Status and Milestones

CyberCoin was operational since October 1996 but as of 1999, CyberCoin is not available anymore. InstaBuy is now offered instead.

2. Availability (access)

Both merchants and customers need an U.S. bank account. For non-U.S. citizen customers a credit card is necessary. The CyberCoins are only available in U.S. dollars and only at merchants who have an U.S. bank account.

3. Convenience

The CyberCash wallet software is needed in order to store the CyberCoins, which could be very tedious to always first download the software. Furthermore, only the merchants with an U.S. bank account accept CyberCoins.

4. Security

Double spending is no issue with CyberCoin since it is not a token system (i.e. no real electronic cash is used), but a notational one. As customers do not need to store any monetary value on their PC, they do not face the problem of loosing money, if their PC crashes and they can access their CyberCoin accounts from other PCs as well.

This system is *not anonymous* as all the transactions can be traced. The wallet will release the CyberCoins to the merchant only after the customer has received the goods. In this way the customers are protected from loosing money due to errors or fraud in electronic transfers.

5. Support of micropayments

CyberCoin supports micropayments.

6. Merchant risks involved

Minor risks are involved as the merchant receives immediate payment after the customer has received the goods. In the case of non-U.S. citizens a stolen credit card can be used to authorise payment, i.e. authorise an amount to be transferred from the consumer's account to the merchant's account.

7.2.3 Evaluation Criteria of the NetCash System

1. Status and Milestones

The NetCash system closed trial in 1996. It was designed for open networks and to issue coins to users of the system, accepting electronic cheques in payment for them.

2. Availability (access)

NetCash is currently not for global use, since customers must have an U.S. checking account to buy or redeem NetCash coins of exact denomination. NetCash provides scaleable electronic currency that is accepted across multiple administrative domains.

3. Convenience

Compared to DigiCash, NetCash does not require any special software to use. If the customers have lots of spare change, NetCash can however become very difficult to handle, similar to the DigiCash system. NetCash does however offer a "change" function where the customer or the merchant can have their loose bills and change consolidated into a higher denomination [60]. Furthermore, NetCash requires correct change for each sales transaction, which is a hassle, while automated. Because of the fact that NetCash coins must be bought in advance and the use of e-mail is also not very convenient, transactions tend to be extremely tedious.

4. Security

Network security is provided using both *symmetric* and *asymmetric cryptography* where all parties are holding their own public-private key [79]. A great deal of the security is however, also dependent on the security of the e-mail system. To prevent double spending and to ensure authenticity, the merchant must check the validity of each coupon received with NetBank.

NetCash provides a weaker form of anonymity than Chaum's DigiCash system [75]. As described above, at the point when a customer purchases coins from a currency server by cheque, or cashes in coins, it is possible for the currency server to record the serial number of each coin. Similarly, when the merchant presents the coin at the server for verification the coin is checked against the list of issued coins. If the coin is present, then it is a valid coin originating at the server [123]. At this time the server knows exactly who has spent the coin and is able to detect double spending. Thus the flow of cash through the economy can be recorded and only *partial anonymity* is guaranteed.

Each coin issued is holding a unique serial number that is recorded by the server, to whom they were given. Although the digital cash is identified with each coin issued, there is an exchange mechanism to provide *limited anonymity* [79]. In order to obtain this variable degree of anonymity, both the customer and the merchant can exchange their valid coins with the minting server for new coins. This prevents the server from storing spending profiles and at the same time guarantees some limited anonymity to the merchant and the customer. If however, all parties collude in the NetCash system, including the currency servers involved in the transaction, it is possible to determine who spent a certificate. It is expected that currency servers will not do so. Any client and merchant gets the chance to choose the NetCash currency server they trust and which will not keep required information to track such transactions.

Whether the anonymous exchange protocol is used or not, the buyer always remains anonymous to the merchant, although the merchant will know the network address. The merchant on the other hand can remain anonymous to the buyer, if he generates and distributes a temporary public-key pair instead of using always the same one.

NetCash uses a *double spending detection system*, implemented in the reverse manner to the DigiCash eCash system [129]. Whereas DigiCash keeps track of all tokens spent, NetCash keeps a list of coins issued and crossing of the redeemed ones. eCash cannot keep a list of issued coins, because of the blind signature scheme ensuring anonymity. The trade-off between NetCash and eCash is determined by the ratio of tokens unredeemed to tokens redeemed. If the number of unredeemed tokens are more than the number or redeemed tokens, eCash requires less overhead. NetCash means less overhead, if the ratio is in reverse order [123].

5. Support of micropayments

NetCash was designed to support mainly information products under $100 but can be used for payments as low as $0.25.

6. Merchant risks involved

Merchants have a choice of either assuming risk and accepting "pending" coupons, or assuming no risk and accepting only "valid" coupons. They do however not receive their payment immediately, because a certain time delay is incurred. Furthermore, they are getting penalties from low-value redemptions. Therefore, in order to avoid this, the merchants always need to accumulate the incurred transaction before they "claim".

7.2.4 Evaluation Criteria of the MilliCent System

1. Status & Milestones

The goal of MilliCent was to provide transactions that are inexpensive yet secure. At the moment it is not a universal system, as each merchant's scrip is only usable on the merchant's web site. The system went live on June 1, 1999 in Japan [44].

2. Availability (access)

Customers do not need to have a bank account, but they must buy scrip before conducting a transaction. The scrip represents an account the customer has established with a vendor.

3. Convenience

Customers need to find a broker that will sell the relevant vendor scrip. Furthermore, an electronic wallet needs to be obtained in order to store the broker scrip. The fact that the scrip is not limited to one standard currency (which could also be an advantage) and every merchant can create its own scrip could make the scrip become merchant-specific. Merchant-specific scrip could lead to scrip leftovers that cannot be used at other sites. Digital has however offered to buy back "leftover" scrip in exchange for new scrip.

4. Security

The security model for MilliCent is based on the assumption that scrip is used to represent small amounts only. As Mark Manasse from MilliCent – DEC states: "Scrip is not worth stealing, unless you can steal lots of it, and if you steal lots, you will get

caught". Therefore, the amounts at risk in a transaction do not present a major drawback. Apart from this, scrip has the following *built-in security features* [35]:

- Tamper-resistance,
- Difficult and expensive to counterfeit,
- Spendable only by its owner,
- Spendable only once, which ensures double spending will be detected by the vendor at the time of the purchase,
- Vendor-specific, and
- Creation of unique digital signatures by using only symmetric cryptography and not public-key cryptography. As public keys take far longer to generate than symmetric ones, they will delay the purchase and at the same time reduce the transaction-processing rate. For micropayment systems to be effective they need to achieve a high transaction-processing rate.

Furthermore, it is assumed that the system contains a *natural antifraud mechanism* and people treat scrip as they would treat change in their pocket. Normally users would hold only a few dollars of scrip at a time. For merchants, the amounts involved are so small, that it's unlikely that any merchant would fail to provide the goods purchased. Brokers on the other hand would not risk their reputations for easily traceable thefts.

As a result of the natural antifraud mechanism assumption, MilliCent makes use of only ligthweight encryption, such as, *symmetric encryption* and a *one-way hash function*. The aim of MilliCent is to make the cost of breaking the protocol greater than the value of the scrip itself (i.e. make the fraud more expensive than a purchase). MilliCent offers three levels of security during transfer [123]. The protocol for the desired level of security can be chosen (listed from the least private):

1) *Scrip in the clear*. The scrip is transferred between the customer and the vendor without any encryption. This means the scrip is traceable and any intruder can copy it in order to spend it.
2) *Secure without encryption*. The customer and the vendor share the customer secret. This secret is appended to a transaction request from the customer to the vendor and

then hashed. The vendor will re-compute the signature from the transaction request in order to verify the validity of the request. This level of security provides no anonymity, as the transaction details are readable by any observer. The security level does, nevertheless, protect against theft.

3) *Private and secure*. The system depends on shared secrets and one way hash functions, guaranteeing privacy. In this case no observer can gain any information.

The scrip in general *does not provide anonymity* [129], because the owner's identity is coded into a field of the scrip. Furthermore, the serial numbers (in the form of ID numbers) that are used to prevent double spending, can be recorded and traced.

5. Support of micropayments

MilliCent clearly aims at the micropayment segment. It uses scrip (similar to cash) instead of real money and is only valid with a specific vendor.

6. Merchant risks involved

The long-term relationship is between the brokers and the customers, and the brokers and the vendors rather than directly between the customers and vendors. As brokers repudiation is important to attract new customers and vendors they would not risk any fraud. There is no risk for the vendor because a digital signature prevents the customer from modifying the scrip's value. It could however be difficult for the vendor to keep up with all the small microcent transactions.

7.2.5 Security Comparison of the Electronic Cash Systems

Below in Table 7-2 the different electronic cash payment models with respect to their security characteristics are compared.

Token.	Notational.	Token.	Token.
Cash like [44].	Account based.	Cash like.	Cash like.
Micropayments.	Micropayments.	Micropayments [129].	Micropayments.
Online.	Online.	Online.	Semi-Online, as some preparations involve the broker as well [129].
Yes. Like true cash, DigiCash can be spent anonymously [92].	No [123]. The banks as well as CyberCash can trace all transactions.	Yes, but limited, due to unique serial number recorded by the server. No anonymity with respect to the NetCash currency server.	No. The broker knows who and where but not what. The vendors know what but not who. Furthermore, the owner's identity is coded into the scrip.
RSA and DES encryption and a cryptographic invention known as "blind-signature" technology.	RSA and DES encryption [129].	Symmetric and asymmetric cryptography are used [79]. Also relies on the security of the e-mail, using an encryption scheme known as PGP.	Hashes & general lightweight security [123].
Yes.	Yes.	Yes.	Yes. Authentic scrip is used.
Yes. The cash includes a serial number and online validation is carried out.	Not applicable.	Yes. Once a bill is used it is permanently removed from circulation, but offline coin transfer cannot detect double spending.	Yes. Vendor validates the unique identifier of the scrip [129].
Bank that supports eCash system (or Mark Twain Bank before 1998).	CyberCash server.	Customer and merchant communicate with currency server.	Buyer trusts broker and merchant. No third party is involved.

Table 7-2 The security profile for the various electronic cash payment systems, based on the information currently available

7.3 Security Techniques provided by Smart Cards

For smart cards to be secure users must bear some responsibility to manage their own smart card. The security policy must clearly specify the responsibilities of each entity as to the use and management of each smart card [4].

A smart card can only be trusted as a secure device if it protects the sensitive information as well as the sensitive applications inside the chip. It must avoid:

- Disclosure of sensitive information stored in the smart card or send via the smart card to the outside world
- Manipulation of sensitive information
- Modification of sensitive information

There are various mechanisms in place to **protect the IC chip**. First of all the circuit chip is overlaid by the printed circuit, which provides connection points for power and data. Second, the circuit chip is made from silicon, which is not easy to break. Thirdly, the size of the circuit chip is restricted to only a few millimetres to avoid breakage when the card is bent. Finally, special layers of oxide over the chip protect against exposure of the memory contents. Another protection against exposure of memory contents is the small electrical charges of an EEPROM. Trying to tap information by raising or dropping voltage levels could lead to the loss of information.

With a smart card, information theft it is practical impossible and fraud is reduced to a great extent. The chip card is designed in such a way that sensitive information is disclosed to nobody but the authorised users, by requiring very specific PIN information. By setting up the **access condition** and password on files, only authorised persons are allowed to access the information. Each file has a header attached, which indicates the access conditions (i.e. who has the right to read, write or erase information on a smart card) or requirements of the file and the file status. Access control is based on the correct presentation of a password, usually in the form of a *PIN number*, ensuring the identity of the authorised bearer and subsequently allowing only authorised persons to access and

use the smart card. After positive identification, the required user actions will be performed by the smart card.

The **access tracking area** of the EEPROM memory is assisting in keeping track of the number of access attempts to secure information with valid or invalid PINs. If more than allowed attempts (depends on the systems) are started the corresponding PIN will be invalidated or blocked.

The various security keys and codes, along with the encryption techniques for controlling memory access, provide a great level of security for the data that is stored on the smart card.

Encryption and **biometrics** are another two approaches ensuring strong security. Any data, passing between the smart card and an external system, and all the data stored on the smart card is encrypted, preventing unauthorised persons from reading the information. This makes smart cards an attractive means for secure information storage. *Digital signing* and encryption of e-mails is also done by the smart card.

The hardware platform of the chip cards is used for secure storage of information and keys, and the execution of applications using sensitive data. For storage of information, such as, private keys, account numbers and valuable personal information, there are three different types of memory (RAM, ROM and EEPROM) on the smart card chip.

Personalisation takes place by encrypting the user data under a cryptographic **personalisation key** that is known only to the owner of the application. This key is installed in the chip during initialisation. Cryptographic operations are performed on the smart card itself, avoiding any key transfer on the insecure network, and reducing fraud.

Smart cards, when used with strong **cryptosystems** store the cardholder's digital signature very securely and provide strong authentication and repudiation. Users must be authenticated before the card can be used. Coupled with **biometric authentication**

methods, which rely on personal physical attributes, smart cards may provide improved security, i.e. reducing fraud and abuse. Biometrics involves the use of finger-scans (electronic fingerprint identification) or eye-scans to identify individuals as indeed being the persons they claim to represent. Therefore, the use of biometrics may provide a final means of absolute personal authentication.

As the smart cards have room for identification they can allow for the return of the card to the consumer if lost. However, as the stored value remains with the card, the cardholder has no longer the resident value if the card is lost. Furthermore, smart cards have privacy concerns, as people think they are storing too much personal data.

For smart cards to be used in future they must rest on standards and industry members must solve interoperability issues. If these issues are resolved, the smart card can be an element of solution to a security problem in the modern world. In order to determine the evaluation requirements provided by a smart card, the Mondex smart card is evaluated.

7.3.1 Evaluation Criteria of the Mondex System

1. Status & Milestones

The concept of the Mondex card was developed in 1990 [79]. The card was designed to be a global payment system and closed trial since July 1995. In July 1996, Mondex International was formed to promote the technology. Currently they license their rights to a local Mondex originator in each country. The originator then creates the cash in the local nation's currency.

2. Availability (access)

Smart cards are available to anyone wanting to use them and can be used both for POS transactions and the Internet. The greatest advantage of the Mondex system is the ability to use it in the real world. The Mondex smart card is portable and able to handle multiple currencies and multiple applications simultaneously.

3. Convenience

The operating system MULTOS (multiple operating system), developed by Mondex, allows for more than one application on the smart card. So, besides Mondex's application of electronic cash, one could also have personal educational records, and one's telephone account on the card. This is advantageous, since it reduces the number of cards one carries. Apart from this, payment can be done via the Internet, at home, at a store or over the phone. No central processing and no authorisation are required, only the two participant cards are involved in a transaction.

These smart cards hold a pre-programmed amount of value. The greatest convenience for the customer is probably the fact that a smart card is easy re-chargeable. Mondex cards can store "value" in up to 5 different currencies, although at present it is not possible to perform currency exchanges between them. In order to use the Mondex payment system, every customer requires a smart card reader, which could yield some constraints.

An advantage over the DigiCash and MilliCent system is that electronic money stored on the Mondex cards can be exchanged for government currency any time at a bank.

4. Security

Mondex has strong security and risk management to prevent, detect and recover from potential counterfeit activities [31]. It provides features, such as, physical security and cryptographical security.

For security purposes, Mondex relies on a unique "digital signature" generated by the chip on the consumer's card, using public-key cryptography. This digital signature is recognisable by the other transaction party, so two Mondex cards can authenticate each other during a transaction. Furthermore, the Mondex system allows monetary value exchange between merchants and customers without intervention of an authorising authority (such as, the bank). Encryption and security is applied to the smart cards and the smart card readers. However, any stored cash balance in the Mondex card is not

protected against loss or theft. If the card is lost or stolen, there is no way to recover the money.

The Mondex transaction trail is *not anonymous*. A limited transaction trail is maintained on each card and on each terminal. The customer's card keeps track of the last ten transactions [158]. Although in principle only the card-issuer is aware of the relationship between the card identifier and the account-holder. Apart from this, the bank can trace all transactions and is able to build customer profiles. The card can be locked with a PIN, which can also be used to trace the owner of the card, in case of loss.

As already mentioned, the Mondex card logs all transactions. It stores the unique customer ID registered at the customer's bank, where the personal information about the customer is stored [129]. This ensures that any lost Mondex card can be returned to his/her owner. To avoid unauthorised usage of the Mondex card, it can be locked using a personal code or passphrase.

5. Support of micropayments

Mondex works much like cash and handles both large and small transactions. Because Mondex transfers occur immediately via the chip-to-chip technology, Mondex eliminates the large infrastructure expenses of the credit card paradigm. That's why it's ideally suited for handling smaller transactions, even under a dollar.

6. Merchant risks involved

The main benefit of Mondex cards is that it carries real cash. This can however be a risk in the case of theft. If it's lost, the value will not be able to be retrieved back. The merchant bears minimum risk as he/she receives immediate value transfer.

7.3.2 Security Profile of the Mondex System

A summary of all the security aspects of the Mondex smart card system is shown in Table 7-3.

	Token.
	Cash-like, i.e. smart cards.
	Micropayments.
	Offline.
	No. Neither purchaser nor seller is anonymous. In some way Mondex is cash. Furthermore, the banks hold user data and can trace all transactions.
	Encryption is applied to smart cards and to smart card readers.
	Yes. The Mondex card generates a digital signature. This signature is used so that two Mondex cards can authenticate each other [129].
	Yes. The unbroken hardware should ensure this [129]. If the owner of the smart card attempts to spend some e-money twice, the chip in the smart card would detect the attempt and would not allow the transaction.
	No third-party intermediary, but value flows from one chip to another.

Table 7-3 The Mondex security profile, based on the information currently available

7.4 Comparison of Debit and Credit Cards Online and Offline

Using the credit/debit transaction model, the credit/debit details are sent from the consumer to the merchant. The merchant, who must be authorised by the issuer, verifies these details with the issuer (normally a third party). Once, the issuer confirms the details, the merchant will send the goods to the user. The transaction is sent to the issuer for settlement, who will debit the consumer's account and credit the merchant's account.

While conventional cheque and credit card systems may seem quite similar, the legal meaning of credit card and cheque payment differ significantly. Credit card companies warrant their merchants and a person may claim restitution from the card-issuing bank, when dissatisfied with the goods. Cheques provide no such recourse – a purchase is unsecured if claiming for dissatisfied goods.

Both the eCheck and NetCheque are very similar to the traditional paper cheques. Digital signatures are used as substitutes for the hand-written signatures found on paper checks and the traditional paper document is replaced by an electronic document. Apart from this, the NetCheque system is also suitable for micropayments, which does not apply to traditional paper checks.

The eCheck is designed to perform the payment of paper checks, by using cryptographic signatures and secure messaging over the Internet. Since the eCheck does not depend on real-time interactions or on third party authorisations, eChecks are better able to survive outages of network links and computing links.

The electronic credit-debit payment systems do not provide a great deal of anonymity but auditability - the payee is always able to track who authorised the payment. The primary prerequisite in transferring the credit card purchase processes to the Internet is that the cardholder's position should in no way deteriorate. At the same time, merchants and credit card institutions must try to minimise their risks. Various transmission protocols, for example SET, have been developed to protect credit card information from prying eyes during transmission. Electronic credit card based payments are secure, when used using secure socket layer, such as, SET, and build on a common infrastructure: credit cards. Due to the central processing costs these payment models are, however, not effective for micropayments.

With conventional credit card payments the merchant captures the customer's credit card data at the point of sale. Depending on the merchant's policy he can check on the card status with the acquirer. This method is not completely secure; the customer may deny and recall an order afterwards. In electronic credit card transactions, the merchant only delivers the goods and/or services once the transactions is confirmed by the payment gateway.

All the electronic cheque and electronic credit card systems are evaluated in greater detail according to certain evaluation criteria.

7.4.1 Evaluation Criteria of the FSTC Electronic Check System

1. Status and Milestones

The FSTC eCheck project was used by the United States Treasury [125] in a two-year pilot program. In June 1998, the first electronic check was sent by the U.S. Treasury department over the Internet [36]. The FSTC's eCheck provided this service. As the eCheck is modelled to resemble the traditional paper cheque, the FSTC Consortium expects that the system will gain acceptance due to consumer's familiarity of the traditional cheque systems. The primary aim of the FSTC eCheck is to make electronic cheque payments possible over public networks [129].

2. Availability (access)

The eChecks are designed to be able to be cashed in by anyone at any financial institution. However, only authorised individuals are assigned a portable electronic checkbook. The eCheck can be used for paying anything, i.e. in every situation where a paper check is used today. The eCheck will reduce the payment cycle compared to the payment cycle of the traditional cheque system.

3. Convenience

eChecks are portable and any bank would honour them, since they are designed to be compatible with the existing financial services information infrastructure. However, for a customer to "write" electronic checks a smart card reader is required.

4. Security

The eCheck incorporates several security techniques, including data encryption, digital signatures, certificates, and secure e-mail and hardware tokens (such as smart cards) to ensure that the security of the system is not compromised. *Authentication* (both, the eCheck and signer are authenticated), *public key infrastructure* and *certificate authorities* are used to ensure the integrity of each electronic transaction and detect any tampering that has occurred while the cheque was "in transit".

The *digital signatures* provide an ability to identify and authenticate the creator of the signature and to ensure non-repudiation.

The *X.509 certificates* are issued to payers and payees through their bank or through their eCheck service provider and are used to enable a payee to determine the validity of the signatures. The X.509 certificate only ensures the signature verifier that the public key was associated with a signer and bank account at the time when the certificate was issued. It does not guarantee that sufficient funds exist in the payer's bank account.

The *electronic checkbook smart card* (or other cryptographic hardware) is used to protect the signer's private signature key from theft and misuse and subsequently to avoid cheque forgery. As the private key is stored in the electronic checkbook and never transferred via the computer's network connection it should not be possible to forge the private key, except if the user's checkbook is stolen or lost. Furthermore, to ensure the uniqueness of each eCheck, the electronic checkbook numbers each eCheck when it is signed. Encryption is not required to prevent fraud, but any information may be encrypted for privacy reasons, using encryption hardware.

Anonymity is not possible as the eCheck contains all the necessary information, such as, the payee's name, the amount, the date and the account information, necessary to process a payment. All this information is maintained on the eCheck in order to complete the transaction without the intervention of an authorising financial institution.

5. Support of micropayments

The eCheck supports only macropayments.

6. Merchant risks involved

Merchants must assume all the risk for bounced checks and they do not receive immediate payment. Apart from this the system is expensive for merchants, as it is not totally net-based.

7.4.2 Evaluation Criteria of the NetCheque System

1. Status and Milestones

The first prototype was available in December 1994. Due to the Kerberos export restrictions, NetCheque is only available inside the U.S. [129]. The NetCheque system reaches a wide domestic audience but it is expensive for merchants as it is not totally net-based.

2. Availability (access)

Payments using the NetCheque payment system originate from *named user accounts*. Therefore, users must be registered with NetCheque before they can make payments.

3. Convenience

As the NetCheque is basically the same as for a paper cheque, the concept of using the system is easy to understand. The NetCheque system clears payments between NetCheque accounting servers, as well as between servers of different types. The currency servers guarantee the interoperability of the system itself. Reliability and scalability are provided by using multiple accounting servers. The fact that a cheque system supports micropayments is of great benefit.

4. Security

NetCheque provides security, reliability, scalability and efficiency. The signatures on the cheques are authenticated using Kerberos. It uses *conventional cryptography* and is well-suited for micropayments.

Security is achieved by *authenticating* the signatures on cheques using Kerberos. A NetCheque is, essentially, a specialised kind of "ticket" created by the Kerberos system. A user's *digital signature* is used to create a single ticket, namely a cheque. The payee's digital "endorsement" creates an order to a bank computer for fund transfer.

With NetCheque, properly signed and endorsed cheques can be electronically exchanged between financial institutions through electronic clearing houses, with the institutions using these endorsed cheques as tender to settle accounts.

NetCheque does not provide *anonymity*, as the cheques themselves are not encrypted and an observer has full view of the transaction.

5. Support of micropayments

The NetCheque system is well-suited for clearing micropayments as it allows writing cheques for relatively small amounts. This requirement for handling micropayments requires high performance, which is obtained through the use of conventional cryptography, instead of public-key cryptography.

6. Merchant risks involved

As users must be registered as a NetCheque user before they can make payments, NetCheque started with a very small initial customer base. The merchants have to bear all risks for bounced checks and they receive payment only after 24 hours.

7.4.3 Security Comparison of the Electronic Cheque Systems

A summary of all the security aspects of the electronic cheque systems are shown in Table 7-4.

	Notational.	Notational.
	Cheque-based.	Cheque-based.
	Macropayments.	Micropayments [75].
	Online.	Online
	No. It fails in the area of consumer anonymity and traceability.	No. Transactions between purchaser and seller can be linked in most cases.
	Public-key cryptography for digital signatures. The private key is stored on the checkbook smart card.	Conventional cryptography, which is needed for the high performance that micropayments require.
	Yes. The electronic checks are authenticated via digital signatures [129].	Yes. The system is based on Kerberos. The authentication information is used as the signature on the cheque.
	Yes. By using smart cards and PC cards as electronic checkbooks the FSTC electronic check will be almost impossible to forge.	Yes.
	In 1998 FSTC issued the Bank Internet Payment System (BIPS) specification in order to provide a trusted infrastructure [36].	Payees and payers accounting server are trusted.

Table 7-4 The electronic cheque systems security profile, based on the information currently available

7.4.4 Evaluation Criteria of the SET Protocol

1. Status and Milestones

SET was released to the public on May 31, 1997 [3] and is designed to operate both in real time, as well as on the World Wide Web and in an e-mail environment. This payment system is growing in popularity, and even plays a role in other electronic payment systems. It does not define any particular underlying traditional payment system and can be used either with debit or credit card. SET uses a secure card presentation notational payment model with online validation and is benefiting from the wide-usage of credit cards.

SET is perhaps the most universal of all electronic payment systems, designed to work with any software or hardware platform. SET is used in Europe and Asia, while failing to make any significant impact in the U.S. or Australia [70]. A study by Forrester Research found that less than 1% of all merchants in the U.S. are using or plan to use SET [94].

2. Availability (access)

As an open standard, SET specifications can be used freely by anyone (consumer, merchant and banking software companies) wishing to develop SET-compatible software for buying and selling on the Internet.

3. Convenience

The SET electronic payment system's biggest advantage is the convenience that it offers:

- No accounts need to be set up, but the cardholders and merchants need to register with the CA before they can use SET.
- No prior relationship is required between the merchant and the customer.
- Very universal as it can be used by anyone, who has a credit card anywhere in the world.
- The system is analogous to a real world payment system, thereby increasing the chances of customer and merchant acceptance.
- Compatible with existing credit card contracts.

However, one disadvantage of SET is that the security algorithms used by the system require a lot of computing power, which requires the use of dedicated servers. This makes the implementation of SET very expensive. Furthermore, if compared to the other systems, SET is hindered by its lack of micropayment support.

4. Security

Encryption processes, such as, the *RSA public key* and *DES symmetric key* cryptography systems [123] are used to ensure a secure transmission of the credit card information within the Internet. The 56-bit key is used to safeguard normal messages. More critical

account information is encrypted by means of 1024-bit RSA encoding and tagged onto the message.

The most important security measure employed by SET is the use of *digital certificates* to verify that both parties, the merchant and the credit-cardholder, involved in a SET transaction, are who they claim to be. At the system heart is a pair of digital keys, one public and one private, held by each party in a transaction. In practice, banks will give both keys to a customer together with a digital certificate for authenticity. When customers wish to purchase over the Internet, they first give the public key to the merchant along with the certificate to prove its authenticity. Merchants and financial service providers also receive certificates so that they can identify themselves to each other. In this way all the parties in a SET payment process will be required to authenticate themselves at some point, ensuring they "know" each other and are proper authorised. Meaning, the certificate stored in *X.509 version* makes an interaction between the identification features (i.e. derived from the credit card number) and cryptographic keys, which are used to digitally sign and encrypt a transaction possible. Therefore, the digital certificates create a *trust chain* throughout the transaction, verifying cardholder and merchant validity.

Furthermore, the certificate can be used as a virtual card, which authenticates that a cardholder is a legitimate user of a branded payment card account [60].

SET uses a technique called *dual signatures* [123] that allows a customer to link two messages cryptographically together in such a way that a third party can verify that the payment request corresponds to a certain offer, without seeing the details of the offer itself. Therefore, the dual signature ensures that the transaction details are confidential, which is very important, as the SET participants are not anonymous.

SET does not ensure a great deal of *anonymity* as both the merchant and the credit card issuer keep detailed records of activity, like in any regular credit card transaction. The

merchant sees the customer only partially, as the customer's account and credit card details are encrypted and only visible to the payment gateway and the bank.

To summarise, the most significant features of SET, covering all the security requirements, are [48]:

- Ensuring *confidentiality* of information, by protecting the relevant transaction data from unauthorised access, through a special encryption procedure.
- Ensuring *data integrity*, using digital signatures or message digests.
- Ensuring *availability*.
- Providing *authentication*. The customer, merchant, and bank must use certificates and digital signatures for *authentication* and in order to complete a transaction. The digital certificates create a trust chain throughout the transaction, verifying cardholder and merchant validity.
- Providing *non-repudiation* through the use of signed digital certificates [191].
- Withholding bank-relevant transaction data from the merchant, using *dual signatures*, guaranteeing absolute security for the customer.

In the CyberCash protocol, only CyberCash knows everyone's public key. In SET, however, consumers, merchants, and acquirers must exchange certificates before a party can know which public key to employ in order to encrypt a message for a particular correspondent. Therefore, there exists a hierarchy of certificate authorities that keep the binding information of a user and a public key.

5. Support of micropayments

SET is not the most popular system to use for micropayments. One reason is the vast amount of messages that need to be exchanged between the customer and merchant.

6. Merchant risks involved

Card issuers must invest considerable sums to have public key pairs and certificates issued to their cardholders. The SET protocol guarantees the merchant payment. But, although merchants face no risk it is not always clear for them that SET will generate

significant new credit card volume, as opposed to merely displacing mail and telephone orders.

Although the possibility of fraud is reduced with the use of a SET-secured transaction, it is still the responsibility of the customer to check his/her credit card statements for unauthorised charges. One problem with SET is the lack of customer identification, as one could easily place a fraudulent order, using someone else's credit card number [60].

7.4.5 Evaluation Criteria of the CyberCash System

1. Status and Milestones

CyberCash was founded in 1994 and processes Internet credit card payments since April of 1995. It is a global system and no U.S. banking presence is needed [79]. According to CyberCash more than one million CyberCash wallets have been downloaded for use in e-commerce and more than 3,000 Internet merchants and hundreds of leading banks are affiliated with CyberCash. CyberCash is the only company with the world-wide export license of 1024-bit RSA encryption algorithm. David Stewart, vice president of Global Concepts says that all major e-commerce sites must use CyberCash in order to be attractive to shoppers. CheckFree, CompuServe and America online have already adopted the CyberCash software.

2. Availability (access)

As the CyberCash payment system accepts major credit cards, it is not necessary for U.S. citizens to have an U.S. bank account to use this system. Users must however, download the electronic wallet after registering with CyberCash.

3. Convenience

The CyberCash system forms a gateway to tie merchants to existing systems like, bank accounts. As CyberCash uses the existing transaction networks it is attractive to the major banking houses. CyberCash ensures that the messages are secured and will be rendered useless if intercepted other than by the intended user. Customers can take advantage of

secure credit card presentation payments, sending their encrypted credit card information to the merchant, ensuring that the merchant never gets to see the credit card number.

4. Security

The CyberCash system has the advantage of *cryptography*, which guarantees security and privacy to the client. CyberCash uses a secure credit card presentation payment model with online validation.

This payment mechanism consists of a downloadable software package using *public-key encryption*, that is designed to assure the security of credit card transactions over the Internet. The fact that all the credit cards used during a purchase must be registered at CyberCash reduces the risk of fraud. When a payment request is not signed by the cardholder's private key a purchase cannot be made. Furthermore, the cardholder's CyberCash ID along with the public key, stored at the CyberCash server, can be used to perform an "emergency close-out" in the case of fraud [79]. As all the financial information (including the customers credit card information) is always encrypted, using CyberCash's public key, the merchant never sees the card data, eliminating a great deal of merchant fraud.

As opposed to the Internet - an open system, all credit or debit card numbers are transmitted over closed-system dedicated banking networks. *Digital signatures*, authenticated by CyberCash, are used by all three parties for authentication and non-repudiation.

Customers protect their privacy, by using their *wallet IDs*, instead of their credit card information, for the purpose of identifying themselves to authenticate a transaction. In this way their credit card information is hidden from the merchants. In the eyes of the merchant, the customer is *anonymous*, with only a deposit appearing in his account. The customer's bank does however receive detailed information of each transaction.

5. Support of micropayments

CyberCash supports only macropayments and not micropayments. The transaction costs are expensive for smaller transactions, since every purchase involves communication to a centralised credit card transaction service.

6. Merchant risks involved

Neither the buyer nor seller is at risk. Once the payment is approved by CyberCash, the payment to the merchant is guaranteed, before any product is shipped [159] to the customer. Customers may however, be unwilling to provide a credit card number (although encrypted) to a vendor they don't know well.

7.4.6 Evaluation Criteria of the FirstVirtual VirtualPIN System

1. Status and Milestones

First Virtual Holdings was fully operational since October 1994, but has abandoned its electronic payment business in July 1998 [44]. The goal was to offer an Internet payment system with the advantage of the e-mail system for messages.

2. Availability (access)

Any user anywhere in the world can set up an account with First Virtual Holdings to receive a VirtualPIN. Sellers receive their funds into a bank account, which must be in an U.S. bank account.

3. Convenience

Although merchants and buyers must have either a bank account or a credit card before they can use the system, they are not required to install new software. Instead, access to Internet e-mail is the key to sell or buy over the Internet using the First Virtual System. Every time a sale is completed, First Virtual Holdings needs to confirm this with the customer, which is very time-consuming and not convenient.

4. Security

First Virtual uses a credit card payment intermediator notational payment model with online validation. VirtualPIN takes advantage of the e-mail system for message exchange between the customer, the merchant and First Virtual. The e-mail system is sufficient and *no encryption* is required, as the credit card numbers are never transmitted over the Internet.

Although First Virtual keeps detailed records of all purchases, which makes the trail of all purchases very clear, they promise to maintain *anonymity*. The customer is however anonymous towards the merchant as the merchant will know the customer only by his/her VirtualPIN, which is a pseudonym.

As this payment system is only used for information items, fraud is not of great importance. Still, attackers can obtain the VirtualPINs by attacking the e-mail system, or they use a stolen credit card to set up an account with Virtual Holdings in order to obtain VirtualPINs. Consumers are however, able to detect this as the company delays payment to merchants for 90 days, which gives them some time to discover fraudulent charges on their credit card statements and allows them to stop any transaction by corresponding with First Virtual Holdings.

One of the weakest points of First Virtual is not using cryptography and therefore, not being able to guarantee total safe transactions.

5. Support of micropayments

Although suited for low to moderately priced information sales, it should be considered that the cost of each credit card transaction and the need for e-mail confirmation from the customer, makes the payment system very costly and slow for micropayment transactions.

6. Merchant risks involved

Although the risk of non-payment is carried by the vendor they are virtually 100% protected from fraud. No charges are processed against their account without their confirmation. One disadvantage of the system is that the settlement process is very long and the merchant gets a delayed payment through an automated clearinghouse, leaving the customer with the product, before paying for it. The credit-card provider is transferring payment to First Virtual after which First Virtual is then transferring payment to the merchants. However, as the cost of sending information electronically "on approval" is negligible, a merchant has little to loose if a consumer's answer is "no".

Confirmation is provided by the e-mail system, which leads to minimal risk. The company relies on the integrity of the Internet's e-mail infrastructure to ensure that a consumer is answering "yes" or "no".

7.4.7 Security Comparison of the Electronic Credit Card Systems

A summary of all the security aspects of the electronic credit card systems is shown in Table 7-5.

Notational.	Notational.	Notational.
Debit/Credit-like.	Credit-like.	Credit-like.
Macropayments.	Macropayments [129].	Macropayments.
Online.	Online.	Online.
No. SET transactions are non-anonymous.	Partial [129]. CyberCash can read the credit card information (but CyberCash is trusted), whereas the merchant cannot. The banks can trace all transactions.	Partial. The merchant knows the customer only by account number. But the transaction is traceable through the bank account that the VirtualPIN is tied to.
Symmetric-key and public-key cryptography. Symmetric key is used for encoding of messages and the power of public-private keys to provide authentication.	DES and RSA encryption [79]. Financial information is encrypted, but the actual message is not. CyberCash uses an implementation of SET.	No cryptography. Credit card numbers are never transmitted over Internet. Takes advantage of e-mail system.
Yes. SET focuses on confidentiality and authentication.	Yes.	No.
Not applicable.	Yes. CyberCash adds a layer of security to the transfer of credit-card information, by using third parties to clear the transactions.	Yes. First Virtual sends an email to confirm before authorising payment.
Yes. Payment card-processing centre or payment gateway.	Yes. CyberCash server links transactions between purchaser and seller (via credit card). Allows the purchaser to remain anonymous to the seller.	Yes. Consumers establish accounts with a trusted third party (i.e. First Virtual).

Table 7-5 The security profile for the various electronic credit card payment systems, based on the information currently available

7.5 Score Evaluation of the Electronic Payment Systems

The various electronic payment systems are compared, as shown in Table 7-6, according to a score assigned to their evaluation criteria. The evaluation criteria used are (with a maximum score of 10):

- Convenience
- Security
- Anonymity
- Micropayment
- Merchant risk protection

	3	9	10	10	10
	5	7	0	10	8
	6	7	8	10	6
	5	9	0	10	10
	7	8	5	10	10
	6	10	0	0	0
	8	10	0	10	0
	6	9	0	0	10
	6	10	8	0	10
	6	7	8	2	8

Figure 7-6 Score assigned to the various payment systems

Convenience takes into account the following criteria (with the number of points assigned to each criteria):

- No special software required (2)
- No need of a bank account (2)

- The cash is not bought in advance (1)
- Dealing with any accumulation of spare change (2)
- Ease-of-use (3).

All electronic payment systems require the consumer to buy the coins/tokens/scrip in advance. For both eCash and CyberCoin a graphical wallet software and bank account is needed. Using the CyberCoin system, the consumer never holds monetary money and therefore, no accumulation of change will occur. This is not the case for the eCash wallet. The fact that DigiCash can be spent at any shop accepting eCash, makes it attractive to use (3/10). NetCash requires an U.S. bank account, but does not require special software and offers a "change" function for the spare change. The use of e-mail is not always very convenient in the NetCash system (2/3). Using the Mondex system, consumers require a smart card reader. Both CyberCash and SET require additional software and a bank account (register with a CA in the case of SET), whereas VirtualPIN requires only a bank account. When using VirtualPIN, the sale has to be confirmed every time it is made (1/3). Both electronic cheque systems require a chequebook. In addition the FSTC electronic check system requires a smart card reader.

The **security** criterion takes into account the following attributes (with the number of points assigned to each criterion):

- The type of cryptography (3)
- Digital signature and authentication support (2)
- Double-spending detection (3)
- Trust in (one) billing server (1)
- Loss of money, due to hard disk crash (1)

For all electronic cash payment systems, except for CyberCoin and NetCash, the risk of losing money due to a hard disk crash applies. Although NetCash offers cryptography and digital signature support, it relies on the security of the e-mail program in use (2/5). The Mondex system meets all security criteria, but if the smart card is stolen there is no way to recover the money. The value flows only from one chip to another without the involvement of an intermediary. For both, the electronic cheque systems and the electronic credit card systems, no loss of money is faced due to a hard disk crash, as no

money is stored in an electronic wallet. The credit card system, VirtualPIN does not provide any cryptography (0/3) and no digital signature and authentication support (0/2), but the system makes use of the e-mail system security. In this case the e-mail system is seen as part of the cryptography support provided (2/3). The electronic check systems (FSTC and NetCheque) incorporate security elements that can authenticate both the cheque and the signer, and detect any tampering that has occurred, while the check was in transit.

DigiCash is the only system that ensures full **anonymity** (10/10) as neither the bank, nor the merchant can track consumer purchases. In payment systems, like NetCash, VirtualPIN and CyberCash, one party (normally the trusted third party or billing server) involved in the transaction is able to track the transaction. These payment systems ensure only partial anonymity and are therefore, assigned eight out of ten. In case of the Mondex payment system, the customer keeps a transaction trail of the last ten transactions, resulting in the last ten transactions not being anonymous.

If **micropayments** are supported the full score is assigned, otherwise a zero is assigned. For example, NetCheque, although a cheque system, supports micropayments. A two is assigned to VirtualPIN, as the system can be used for low to moderately priced information sales. The payment system relies on an e-mail system compared to CyberCash, which depends on a centralised credit card institution.

Merchant risk protection depends on whether the merchant assumes any risk during the transaction and/or whether he receives some penalties. For eCash, MilliCent, Mondex, CyberCash and the SET protocol the payment for the merchant is guaranteed, whereas for the CyberCoin, NetCash and VirtualPIN system the merchant receives a delayed payment. Apart from this, the merchant receives penalties for low-value redemptions when using the NetCash system. Using one of the two electronic cheque systems, the merchant assumes all the risk for bounced checks (0/10).

7.6 Applicability of the Payment Systems

When using credit cards and cheques, the bank plays an important role. For credit cards a bank account is needed, whereas cheques must be exchanged for money at a bank. Most people in the rural areas do not have a bank account and for most of them the next bank is not in walking distance. These requirements make **traditional money** more feasible than cheques and credit cards for people in rural areas and/or in third world countries.

Traditional credit cards are mostly used for larger transactions and by a big percentage of the population in the world. The same population, which is using traditional debit and credit payment methods will most likely be willing to use the electronic equivalents.

In order to use electronic payment systems people must be in the possession of a personal computer and a bank account. For countries like, South Africa, India and Bangladesh, for example, most likely only people in the upper class can afford a personal computer. Apart from this, Africa (and any other third world country) remains far behind the developed world in terms of Internet connectivity and usage, due to the inadequate telecommunications infrastructure. In Thailand where only 2% of the population are accessing the Net (compared to Singapore with a 40%), channels, such as, the phone, fax and a customer visit are important transaction channels in order to reach a customer. It is therefore, clear that for countries with no proper telecommunication infrastructure and/or no Internet access, electronic payment systems, independent of whether electronic cash or electronic credit cards, will not be dominant (not in the near future).

Other equally valid explanations of why the Internet is not used for online shopping and hence why no electronic payment systems are required are: people with no Internet connection or people who have simply not encountered the need to do online shopping,

Convenience is a paramount importance of electronic payment systems. **Electronic cash** proved to be less convenient as people need to buy electronic currency (in the form of tokens, coins and scrip) and need an account (except for MilliCent) at the respective

bank. Furthermore, for all except NetCash, additional wallet software is needed. It seems that e-cash systems have difficulties to gain market acceptance and are not as successful as they were expected to be, as two systems have failed already. DigiCash filed for bankruptcy, whereas the CyberCoin has been replaced with a product called InstaBuy. People tend to rather open their purse for money than to buy tokens. Although DigiCash is not in use anymore, the "blind signatures" technology invention will most likely have profound effects in future electronic cash development.

According to Weinberg electronic cash crashed! He states that for any electronic cash system to become popular, it has to be an improvement over the way customers are buying now and this has not been the case with electronic cash [104]. In order to promote the usage of e-cash, an adoption of e-cash has to provide advantages for the consumer, the shopper (i.e. a shop which can accept e-cash) and the e-cash issuer.

Based on the facts raised, it can be assumed that MilliCent is the best electronic cash system, as it provides for real micropayments. One problem is however that no anonymity is offered. The question is however, whether anonymity is really necessary if payment values are normally in the range of $5 and $0.001? Would people really mind if their transactions were traced if they only buy a newspaper for a few cents?

There is no e-cash service that cannot be provided by an electronic credit card or an electronic cheque. E-cash can allow payees to receive payment immediately while credit transactions have to wait for payment from the credit card company. E-cash is thus closer to actual cash than credit card transactions. It is most likely that e-cash must obtain the same acceptance as real money, otherwise credit cards will be a more convenient payment mechanism for consumers.

Electronic cheques provide an alternative to using credit cards and electronic cash. To be able to use electronic cheques a consumer must register with a third party account server and register a credit card of bank account to the e-cheque facility. Whether consumers will use electronic cheques or electronic credit cards depends on their own

personal preferences. In both cases a bank account is needed and the payment process works in the same way as the traditional way.

From my point of view **credit cards** represent the majority of online payments, because people are familiar with them and merchants avoid the expense of a paper invoicing system. According to Jupiter Communications, in the year 2002, 99% of online transactions will still be made with credit cards [104]. Most of the credit card payment systems require a consumer to download software and wallets and register with third parties and certification authorities. This is inconvenient for consumers and difficult for inexperienced Internet users. Furthermore, the biggest problem perceived by mostly those people who are not using their credit cards is the communication security that makes them reluctant to submit their credit card data over the Internet. Companies must have a security mechanism in place in order to solve this problem and ensure secure transmission of the credit card data over the Internet. One approach could be to employ the SET protocol system.

People shopping online have until today no guarantee that those communicating with each other were actually who they claimed to be. Nor do they have any guarantee that messages would reach the recipient, or that they hadn't been altered somewhere along the way. SET solves these problems by allowing people to shop using a SET certified payment card. SET ensures that consumers are protected from theft of credit card numbers, prevents the merchant from seeing the number, while at the same time providing assurance that the card is valid.

As the SET protocol brings along some disadvantages it is still unclear whether it will really gain world-wide acceptance and/or will be used by merchants on their sites. David Stewart, vice president of Global Concepts [104], predicts that SET will never officially die because the credit card companies have invested too much money in it.

The security concerns that individual cardholders have, could change from country to country. For example, in the U.S., any fraud resulting from online shopping with a credit

card is protected, whereby the cardholder is liable only for the first $50 of a fraud [2]. In Australia, South Africa and Germany the cardholder is responsible for the full amount of the fraud until the card is reported stolen. It is clear that the cardholders would be more concerned about security measures in, for example, Germany than in the U.S.

Smart cards will be mostly accepted in countries where consumers and businesses do not trust cheques and other debt instruments, or where there is a high incidence of inflation, fraud, crime and other factors favouring cash. In North America, for example, smart cards are less accepted by the public due to the popularity of cheques and credit cards. In the year 2000 only 65 million smart cards were in demand in North America, compared to 890 million in Europe, Middle East and Africa, and 485 in Asia [164].

Smart cards are more reliable than cash as a thief can easily use cash. If smart cards have identification pictures on them and require passwords, as a means of authentication, they are a lesser target for a thief. Although credit cards can also have identification pictures, they can be stolen and used online. The strength of the smart card is that the funds availability does not need to be verified like in the case of a credit card and the smart card is suited for low-value transactions. Disposable cards can be anonymous, whereas the anonymity for rechargeable cards can be compromised in a number of situations. Transactions using anonymous cards will not be more traceable than cash transactions.

Smart cards can be used in the offline as well as in the online world. For smaller amounts (for example paying for telephone, taxis and road pricing) they are a good alternative to cash, but for larger amounts, people would tend to use their credit cards (whether traditional or electronic, depends on every individual) instead.

People in Germany are using a smart card (called "Geldkarte"), which is mainly used when buying, for example, groceries. What the people dislike about smart cards is that the balance on their smart card is visible to other people, for example in a shopping queue when a payment is conducted. As soon as the smart card is used, the balance is displayed

on the smart card reader and is visible to anybody who can read the smart card reader. Due to this fact people prefer cash above smart cards.

As smart cards offer an infrastructure that combines the functions of purses, credit cards, ID cards, tickets, coupons and tokens with data for personalised settings, they are here to stay for a longer time. If smart cards do not prove to be usable as electronic payment systems, they will definitely be used in some other areas in our daily lives due to their wide range of applications offered. As a means of identification would probably be one application area, for which they will be used in future. If smart cards are successful in the identification application they could replace the traditional identification applications. Printed information and photographs can be stored in the smart cards. In order to verify this information a card acceptor device will be used. The access control on the cards will prevent unauthorised persons to use the card.

It is unlikely that traditional cash payment will die out, because of its ease of use, flexibility, anonymity, and robustness in the face of technical difficulties. Cheques and credit cards are more likely to be replaced by their electronic counterparts, as the payment process has not changed in the online world.

The **electronic payment systems**, whether cash, credit or debit will depend on the **traditional payment systems** that are widely used within every respective country. For example, in Thailand ninety per cent of non-cash payments consist of cheques [51]. When moving to electronic payment methods, the chance that Thailand will focus on the electronic cheque counterpart is most likely.

Currently it seems that consumers are slow in the "move" towards electronic payment systems. But maybe in the near future the adoption of electronic payment systems will become a reality. Time will tell!

7.7 Conclusion

Looking at the tremendous growth in the world-wide Internet population it is clear that the e-commerce environment needs some payment methods other than the conventional ones. As the technology changes so fast, electronic payment systems, which are used today may be outdated by tomorrow. Which of the above systems will exist in future is not clear, but at least they provide a start towards shifting from traditional to electronic payment. Flexibility of alternative payment mechanisms is needed in order to offer consumers and businesses choices among payment methods and payment risks. For sure there will not be only one single payment system in future – cash, debit and credit systems are needed. The choice will lie with the consumer.

Chapter 8

Conclusion and Future Research

8.1 Introduction

Chapter 1 formulated three research questions based on the research problem:

1) Identifying the most commonly used payment systems.
2) Identifying the security techniques that exist up to date.
3) Compensating electronic payment systems for the conventional payment systems.

The conclusions reached during the research project suggest the following solutions for these questions.

(1) **Identifying the most commonly used payment systems.** Chapter 5 (Traditional Payment Methods) and chapter 6 (Electronic Payment Systems) discussed the various payment systems that exist today. The results from chapters 5 and 6 were combined in chapter 7 (Traditional Payment Methods versus New Internet "Money"), comparing the traditional payment systems and electronic payment systems in general according to their security aspects. Furthermore, the electronic payment systems were compared according to some evaluation criteria. Chapter 7 concluded with a summary that indicated the applicability of the electronic payment systems.

(2) **Identifying the security techniques that exist up to date**. Chapter 4 (Security Aspects) emphasised the most important security techniques, which exist and are used in the various payment systems. Their applicability becomes clear in chapter 5 and chapter 6 when the various payment systems were discussed. In order to understand why these security techniques are needed, chapter 4 also emphasised on the various security risks and threats that are faced today.

(3) **Compensating electronic payment systems for the conventional payment systems.** Whether electronic payment systems will replace traditional payment systems will depend on three (inter-related) factors:

a) The evolvement of *Internet connectivity* in third world countries.
b) The *acceptance* of the electronic payment systems, which greatly depends on the *security* offered by such payment systems.

The Internet requires an accessible telecommunication network. In countries (especially third-world countries) where this telecommunication network has been unavailable, people are unable to access the Internet and the Internet-based e-commerce applications have been limited. Channels must be provided according to customers needs and depending on the infrastructure of a country. Therefore, as electronic commerce development and growth is not equally strong in all countries, the need for electronic payment systems will not be dominant.

Apart from this, the evolvement of e-commerce (chapter 3), and consequently the electronic payment mechanisms (as discussed in chapter 6) on the "Information Highway", will depend on the security mechanisms (chapter 4) in place to control any transfer value.

8.2 Directions for Future Research

One area of possible future research could be related to weighting the level of anonymity needed, in order to make electronic payment systems secure, and the level of anonymity allowed. The degree of anonymity that will be provided in future in an electronic payment system, might depend on the legal policy of a country, as governments are more anxious to limit privacy and security. For example, some countries might allow only conditional anonymity in payment, meaning anonymity may be provided, but at the same time must be revocable by a trusted third party. Another example could be that unconditional (or full) anonymity is only allowed on low value transactions.

Given the rapid evolvement of e-commerce, a further research study would be human interaction with electronic commerce in the future, i.e. is the Internet seen as a new medium for transaction exchange and as a new delivery channel?

New technologies might evolve, that are not comparable to any paper analogue. These technologies could be an ideal topic for further research as these new technologies would uncover new ways to distribute risk, liability and cost among the parties of a transaction. One thing is clear, the research in this field has to be kept current – information relevant today may be inappropriate tomorrow.

8.3 Conclusion

This paper endeavoured to describe the necessity of security in electronic payment systems. With the increased network connectivity available today and the development of secure transaction processing, a great deal of growth is expected in **electronic transactions**.

Before the growth in electronic transactions can really take-off, a secure and trustworthy network infrastructure, that supports the e-commerce communication, is needed. Furthermore, **trust** needs to be instituted between transaction partners and information, and **security** is probably the easiest way (i.e. the most important issue) to achieve this trust. Use of the Internet for conducting electronic transactions does not eliminate the requirements for the sort of security needed by more conventional businesses:

- Physical security
- Enforcement of business procedures
- Anonymity features for protecting privacy
- Confidentiality (keeping messages secret through the use of encryption)
- Integrity (ensuring that a message has not been altered in any way)
- Authentication (proving that the sender of a message is really the person who sent the message)

- Non-repudiation (preventing parties involved in a transaction, denying their involvement)

Although a lot of **security technologies** exist to make the Internet more secure and to ensure non-repudiation transactions, any secure architecture or design will have weak areas. No system is 100% secure. Statements, such as, "our firewall is ensuring that we are secure" or "our site uses 128-bit encryption to ensure the security our customers' personal data", are always flawed. The main consideration in determining whether a system is secure or not depends on whether the level of security can meet the requirements of the system.

Every company has the choice as of which security technology to use, whether virtual private networks, firewalls, cryptography, digital certificates, digital signatures or data encryption to protect their data while in transit. Authentication and non-repudiation confirm the identity of all parties participating in the electronic transaction and guarantee that the transmissions remain private between sender and receiver. The integrity of the transmissions must not be compromised, i.e. all parties must feel confident that no one has altered the message content. Encryption and authentication technologies used in electronic cash payment systems protect the cash payment systems against data loss. VAN's prevent the external party connection to an organisation's computer environments. Cryptography is the foundation on which virtually all Internet commerce security solutions are built and provides an effective means of satisfying the trust needed by e-commerce by providing:

1) Certificates for authenticating people, services, applications, and for access control.
2) Data encryption for confidentiality.
3) Message hashing to provide data integrity.
4) Digital signatures to ensure non-repudiation.

All the electronic applications, such as, electronic mail, electronic commerce, home shopping, Internet banking and share market transactions, replacing some of the

traditional applications, are provided, using the distributed network environment, such as, the Internet (and therefore, the WWW).

This study clearly points out the existing **traditional** and **electronic payment systems**. Each conventional payment technique has an electronic counterpart. For all these payment mechanisms relevance to the customer, ease of use, costs and finally trust will decide the payment mechanisms fate. As with any payment scheme, success depends on consumer acceptance. Any system backed by big-name banking organisations will easily build consumer trust. Schemes that have originated in universities are unlikely to be adopted, unless they can be taken up by financial organisations known to and trusted by consumers.

The electronic payment mechanisms have been classified as **token** or **cash, debit** and **credit**. First came the ATM, then the credit card system, which is now becoming payment tools for the direct debit and finally the smart card. One of the ways the numerous technical solutions for realisation of digital money differ from one another is the degree to which they emulate the properties of real money in electronic payment.

Credit card and electronic cheque systems are convenient (i.e. do not vary from the traditional payment systems) and don't ask customers to change their usual purchasing methods. In both cheque and credit card payment systems the hand-signature is replaced by a cryptographic digital signature. The traditional paper cheque is simply replaced by an electronic document and the traditional plastic card is replaced by a digital version in the form of a certificate. Electronic cash is a little less convenient because customers have to buy electronic currency before they can use it. However, electronic currency also brings a certain amount of privacy to electronic purchases.

SET forms the basis of the trust platform for the use of credit card transactions in electronic commerce. The system is analogous to a real world payment system, thereby increasing the chances of customer and merchant acceptance. SET is benefiting from the

wide-usage of credit cards. Although some countries are still implementing SET, the purpose behind SET is the ability to trade internationally.

A competitive battle is raging between conventional and electronic payment mechanisms, and even among the various new payment schemes. It is likely that not one single system will dominate the market, as there are conflicting requirements for different forms of commercial transactions. With micropayments, efficiency and speed are dominant factors. With macropayments, security is more important than for micropayments, as the gain from fraud tends to be bigger.

Trade-offs, such as, security, risk, cost, complexity, responsiveness, and the time until the transaction is completed, determine the acceptance of a traditional payment system. The electronic payment methods (i.e. electronic cash or electronic credit or debit system) must achieve the same acceptance criteria that traditional payment systems achieved in order to achieve the acceptance that traditional cash has achieved. To see which electronic payment system will be used in future the market will determine the most desirable combinations of *security*, *functions*, *price* and *performance*.

The faster the rate of growth of Internet commerce, the more important safety will be, in terms of both systems defence and business enhancement. As absolute security is nearly impossible to achieve it is important that *proper security controls* are implemented in order for these electronic payment systems to gain customer acceptance. For electronic payment systems, and consequently e-commerce, to be successful, consumers must feel comfortable about *privacy* and they must be convinced that the digital payment mechanism is as reliable as the use of the traditional payment mechanism is today. They must know that they are in control over their transactions and that their transactions are protected from eavesdropping and fraud.

Once the security issue is resolved, electronic commerce will flourish even more!

Appendix A

Biometric Devices

According to Marcella, Stone and Sampias [65, page 111], the following advantages and disadvantages can be identified for the various biometric devices.

Biometric Device	Advantages	Disadvantages
Eye Recognition	Research has established without a doubt the uniqueness of retinal and iris patterns.	Scanning devices are bulky, invasive, and time-consuming.
Facial Verification	This is how most human being identify one another. It is a natural, non-intrusive identification method that will work on just about anyone.	Expression variations contribute to difficulties in using facial verification.
Vocal Identification	People are most comfortable and familiar speaking into a device in order to identify themselves.	Not as accurate as other methods. For example, if somebody has a cold. Furthermore, this identification tends to reject genuine users due to background noise.
Written Verification	One of the cheapest biometrics available. Authorised users can sign a document via an electronic writing tablet and "seal" it, so it can be viewed but not tampered with.	The risk of inaccuracy must be reduced in order to gain market acceptance.
Hand Reading	Hand geometry systems measure the shape of the hand, which makes it ideal for industries where hands may be dirty, or scarred.	Very bulky systems and less accurate than fingerprint systems.
Finger Print System	These systems read the unique pattern of lines on the tip of a finger.	Other biometric devices and security devices, such as, card systems, might be cheaper.

Appendix B

Projection of Internet Online Users

1. An *estimate* of the world-wide Internet population in November 2000 compared to January 2000 is shown in Table B1. It should be noted that different sources present different estimates even in the same time frame.

	November 2000[1]	**January 2000**[2]
Africa	3.11 million	2.1 million
Asia/Pacific	104.88 million	40 million
Europe	113.14 million	70 million
Middle East	2.40 million	1.9 million
Canada & USA	167.12 million	120 million
Latin America	16.45 million	8 million

Table B1 Estimate of world-wide Internet population

2. According to the information found on the CommerceNet Research homepage,[2] the world-wide Internet population is as follows:

a) Computer Industry Almanac[3] reports an expected

- 259 million Internet users world-wide at the end of 1999.
- 349 million Internet users world-wide at the end of 2000.
- 490 million Internet users world-wide at the end of 2002.
- Over 765 million Internet users world-wide at the end of 2005.

b) Computer Economics[4] reports an expected

- 213 million Internet users world-wide by 2001

---

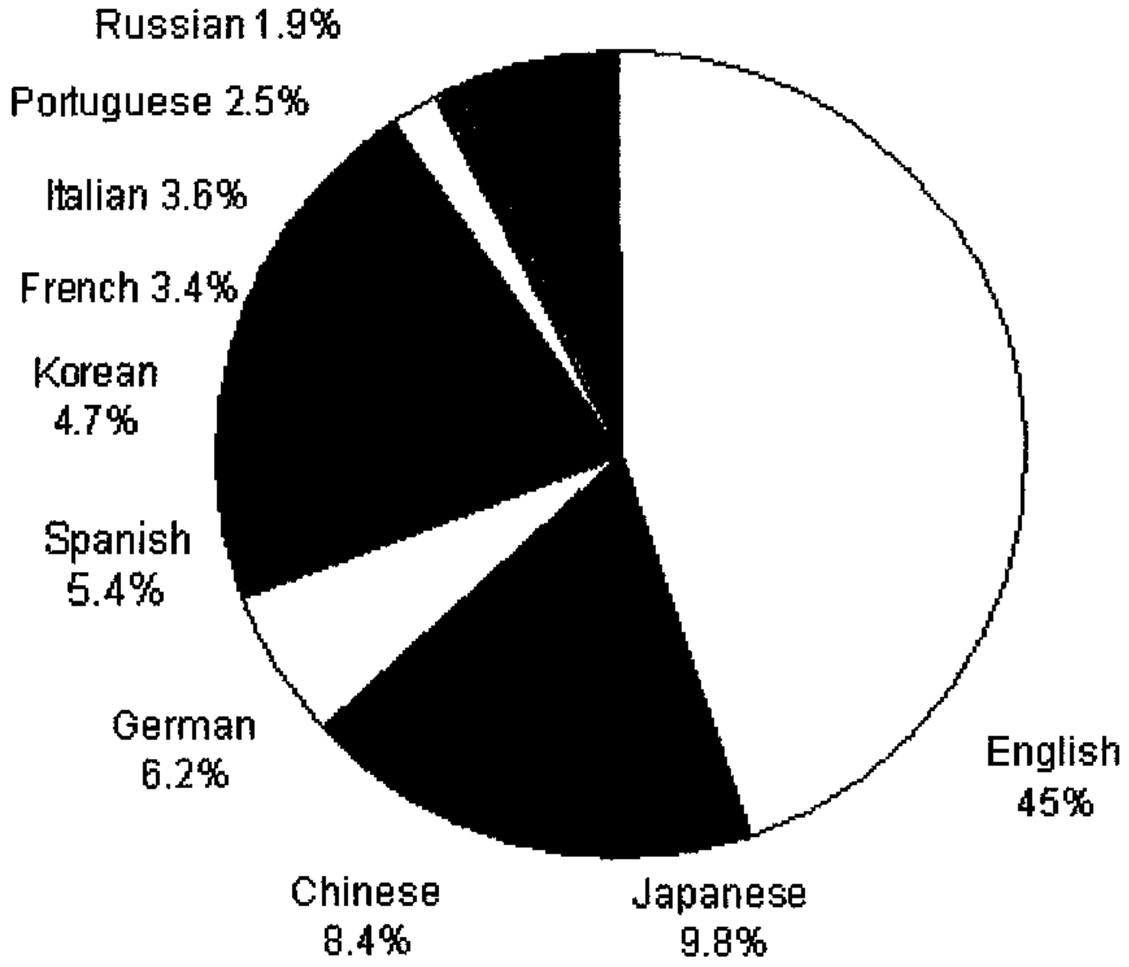
[1] According to NUA, URL: http://www.nua.ie/surveys/how-many_online/

[2] According to CommerceNet, URL: http://www.commerce.net/research/stats/stats.html.

[3] Source at URL: http://www.c-i-a.com/

[4] Souce at URL: http://www.computereconomics.com/

3. According to Global Reach,[5] the latest estimated figures (June 2001) of the number of people online in each language zone (native speakers) are summarised in Figure B1.



Figures B1 Online Language Populations (June 2000)

[5] Source at URL: http://www.glreach.com/globstats/

Appendix C

E-commerce Growth (in U.S. dollars)

Forrester Research[1] says that consumers spent about $7.8 billion online in 1998 and predicts that by 2004, online e-commerce will reach **$6.8 trillion**. This projection includes, both business-to-business and business-to-consumer transactions online and is shown in Table C1.

	2000	**2001**	**2002**	**2003**	**2004**
Total	657.0	1,233.6	2,231.2	3,979.7	6,789.8
North America[2]	509.3	908.6	1,495.2	2,339.0	3,456.4
Asia Pacific[3]	53.7	117.2	286.6	724.2	1,649.8
Western Europe[4]	87.4	194.8	422.1	853.3	1,533.2
Latin America	3.6	6.8	13.7	31.8	81.8
Rest of world	3.2	6.2	13.5	31.5	68.6

Table C1 E-commerce growth - (Totals may not equal sum of rows due to rounding)

[1] Forrester Research Inc., homepage at URL: http://www.forrester.com
[2] North America consists of United States, Canada, Mexico.
[3] Asia Pacific consists of Japan, Australia , Korea, Taiwan, All other.
[4] Western Europe consists of Germany, UK, France, Italy, Netherlands, All other.

Appendix D

Threats Analysis with Preventive Measures

Some general prevention measures against fraud in electronic money systems include:

- Devices containing secret or sensitive information that provide protection against analysis and non-authorised changes.
- Cryptography, which is used to authenticate transactions and devices and to protect data confidentiality and integrity.
- Load transactions that are authorised online by the issuer.

The following table provides an overview of the threats and fraud risks, identified according to Keen [48, page 101].

Vulnerabilities	Threats	Consequences	Preventative Measures	E-commerce Consequences
Modification of data, software and or messages	Manipulation of source data. Manipulation of message traffic in transit. Creation/duplication of electronic notes	Loss of information. Compromise of business transactions.	Data and software are stored in tamper-resistant devices. Digital signatures. The issuer cryptographically certifies electronic notes. Transactions are authorised online.	Mispresentation of information. Reduced legitimisation of information. Potential dispute issues.
Penetration	Impersonation of legitimate users. Data forgery.	Misrepresentation of user. Belief that false information is valid.	Authentication. Encryption.	All of the above.

Vulnerabilities	Threats	Consequences	Preventative Measures	E-commerce Consequences
Masquerading and sniffing	Eavesdropping on the network. Theft of information from source and destination. Information about which source talks to destination.	Loss of information. Loss of privacy.	Authentication. Encryption.	Violation of customer privacy resulting in legal repercussions. Compromise of relationship trust.
Denial of Service	Killing source or destination requests or processes. Flooding machine with bogus requests or processes. Filling up disk or memory.	Disruptive. Annoying. Degradation of service levels.	Firewalls.	Customer dissatisfaction. Violation of service-level agreements. Reputation for poor quality service.
Repudiation	Repudiation.	Violation of non-repudiation.	Transactions are logged by the issuer. Transactions are identified by sequence numbers and are time-stamped. Transactions are cryptographically signed by clients and merchants. CA maintains a database of certified public cryptographic keys.	Compromise of relationship trust.
Cryptographic attack	Theft of cryptographic keys.	Loss of privacy.	Secret keys are generated in a highly secure environment. Any secret keys transported over the network are encrypted.	Private key does not belong to initial signer. This leads, for example, to "false" transactions.

Appendix E

Primary Security Issues

According to Greenstein [36, page 228] the primary security services are divided into five categories. A summary of the five primary security services along with their objectives and techniques used to ensure that they are meet, is illustrated in Table E1.

Security Issue	Security Objective	Security Techniques
Confidentiality	Privacy of message	Encryption
Message Integrity	Detecting message tampering	Digital signatures Hashing (Digest)
Authentication	Origin verification	Digital signatures Digital certificates Passwords Biometric devices
Non-repudiation	Proof of origin, receipt, and contents (sender cannot falsely deny sending or receiving the message and/or transaction)	Digital signatures Transaction certificates Time stamps Confirmation services
Access Controls / Authorisation	Limiting entry to authorised users	Firewalls Passwords Biometric devices

Table E1 Primary security issues with their respective security techniques

Appendix F

Selected Internet Addresses for Online-Shopping (E-commerce solutions)

A few of the successful e-commerce sites are listed and discussed briefly below. These organisations are seeing results from their Web investments.

Amazon.com (http://www.amazon.com)

Amazon.com was founded on the World Wide Web in 1995 by Jeff Bezos a financial analyst, who had no idea of book business. Amazon.com provides a great deal of information about books and allows a search of books by book name, author name and ISBN number. If a book is not found a list of similar books in that category are displayed. Finally, the books can then be purchase online.

AUTOBYTEL Com Inc (http://www.autobytel.com)

AUTOBYTEL is an online automotive commerce company that connects buyers and sellers together. Online customers can research pricing, specifications and other information regarding new and pre-owned vehicles and can purchase, finance, lease, insure, sell or maintain their vehicles. Consumers can purchase new vehicles as well as pre-owned vehicles.

Boeing Company (http://www.boeing.com)

Boeing Company is one of the biggest companies in the aerospace industry, manufacturing commercial jetliners and military aircraft. This company established an Internet site that enabled its customers to order critically needed spare parts. Any Web site visitor can buy travel accessories, gift ideas, aircraft models and posters, books and videos. In 1998, Boeing reported that it received $100 million in orders of spare parts through its web site.

Charles Schwab & Co. (http://www.schwab.com)

Charles Schwab Corp. is the largest U.S. discount and Internet brokerage, offering low-priced online trading opportunities to investors' world-wide. This site provides you with background information and news about a company, examines its finances, read opinions about its performance and, with a couple clicks of your mouse, allows you to buy shares. The Charles Schwab Corporation (CSC) and its subsidiaries provide securities brokerage and related financial services for 7.6 million active client accounts. Client assets in these accounts totalled $805.8 billion at March 31, 2001.[1]

Cisco (http://www.cisco.com)

The world-wide leader in networking (or put differently a telecommunications equipment manufacturer for the Internet), provides open access to its' resources, information, and systems. It sells 70% of its revenues through e-commerce. In 1998, one of its customers bought $100 million of its products without a single human contact.

Dell Computers Corp (http://www.dell.com)

Sells computer products over the Internet. This company has 50% of its business with customers over the Internet.

E*TRADE Group, Inc. (http://www.etrade.com)

This company is a leading provider in online investing services. It offers online personal financial services, such as, value-added investing, banking, research and educational tools and customer service. Since 1992, it has been offering secure, online stock and options trading to independent investors.

Financial Times (http://www.ft.com)

When starting to enter the cyberspace in May 1995, they first only relied on advertising as an income. The top five daily news stories were published on the Internet. Later they

[1] Source: From Quarterly Report (SEC form 10-Q), May 14, 2001.
<http://biz.yahoo.com/e/010514/sch.html>

sold republication rights to customers. This was achieved by transferring all the data to the web site and then allowing customers to download and buy the material from the respective web site at any time. The Financial Times does however retain copyrights of all material [105].

General Electric (http://www.ge.com)

General Electric develops, manufactures and markets a wide range of products for the generation, transmission, distribution, control and utilisation of electricity. In 1997, General Electric purchased approximately $1 billion worth of supplies using the Internet. Using the Internet as a procurement system they realised they have a 50 percent reduction in the purchasing cycle. Furthermore, they had a 30 percent reduction in the processing costs of their procurement cycle [36].

McAfee.com Corporation (http://www.mcafee.com)

Through its Website, the Company allows consumers to secure, repair, update and upgrade their PCs. Apart from purchasing the McAfee antiviral software, they can scan their PC for viruses, clean infected files and perform automatic .dat updates. McAfee.com's applications allow its subscribers to manage their PCs by checking for and eliminating viruses, optimising PC system performance, repairing problems and updating outdated software.

Microsoft Expedia (http://www.expedia.com)

Internet users are allowed to purchase airline tickets and holidays (i.e. packages and cruises), make hotel and car reservations and get exchange rates. Furthermore, the site allows you to find destinations in terms of addresses, businesses, and places, and get *driving directions.*

Motorola (http://motorola.com)

Motorola gathers customer needs for a pager, transmits them to the manufacturing plan, manufactures a specific model (according to the users needs i.e. colour, features etc.) and sends it by overnight mail.

PG Music (http://www.pgmusic.com)

This Web page allows the download of jazz music for several days after payment. The music is delivered as notes on a piano keyboard or guitar and as the music itself. Payment is simply done by credit card.

Travelocity (http://www.travelocity.com)

Travelocity was the first full-service online system. The system is 24x7 hours available and is used by consumers who need to make real-time travel arrangements. The site provides online booking for air, car, hotel, cruise, and vacation reservations.

Virtual WineYards (http://www.virtualvin.com)

This site offers wine shopping online. Furthermore, Virtual WineYards allows buyers to search for wines by brand, vintage, vineyard, rating and price, review winemakers note and view wine labels. Finally, they provide buyers with information on what wines (red or white) to serve with different foods or whether to buy California or French Champagne.

References

[1] **Adams** C. *Piloting Public-Key Infrastructure*. Internet WWW page at URL: <http://www.fcw.com/ref/hottopics/security/PKI.html> (visited April 2001).

[2] **Anderson**, J. Shopping Over The Internet Not so UnSETling After All, *Internetweek*, 18 January 1999. Pages 28-29.

[3] **Asokan** N., Janson P.A., Steiner Michael, Waidner Michael. The State of the Art in Electronic Payment Systems. *Computer*, Volume 30, No. 9, September 1997. Pages 28-35.

[4] **Baker** Richard C. An analysis of fraud on the Internet. *Internet Research: Electronic Networking Applications and Policy*, Volume 9, No. 5, 1999. Pages 348-359.

[5] **Barnard** L., von Solms R. A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. *Computers and Security*, Volume 19, No. 2, 2000. Pages 185-194.

[6] **Barnett** Steve. Top 10 Challenges to Securing a Network. *Network Security*, Volume 2000, Issue 1, January 2000. Pages 14-16.

[7] **Bassham** Lawrence E., Polk Timothy W. *Threat Assessment of Malicious Code and Human Computer Threats*. October 1992. Internet WWW page at URL: <http://www.it.kth.se/~cwe/wastebin/threat-assess.html> (visited June 2001).

[8] **Bennet** David. *Authorisation and Security Systems for E-Commerce*. Internet WWW page at URL: <http://www.it.murdoch.edu.au/~smr/honours/admin/info/DavidsProposal.html> (visited August 2001).

[9] **Bernard**, Cavitt, Mitrey, Scheer, and Sriphetcharawut, *Electronic Payment Systems*. Internet WWW page at URL: <http://jujubee.cob.ohio-state.edu/~scheer/eps.htm> (visited January 2001).

[10] **Berst** J. "Electronic Breakthrough. Finally, an Easy Way to Pay Online". *PC Week*, 16(24), June 14, 1999.

[11] **Blatchford** C. Information security, business and the Internet – Part 1. *Network Security*, Jan. 2000. Pages 8-12.

[12] **Brown** Arlene. VPNs: Only Part of the Remote Access Security Solution. *Network Security*, Volume 2001, Issue 1, 1 January 2001. Pages 12-14.

[13] **Buck**, Peter S. From electronic money to electronic cash: payment on the Net. *Logistics Information Management*, Volume 10, No. 6, 1997. Pages 289-299.

[14] **Cave** A. *Electronic Payment Systems*. Internet WWW page at URL: <http://internet.ggu.ed/~acave/eresource.html> (visited January 2001).

[15] **Chan** Siu-cheung Charles. *An overview of Smart Card Security*. Internet WWW page at URL: <http://home.hkstar.com/~alanchan/papers/smarCardSecurity/> (visited May 2001).

[16] **Chaum** David. "Digital Signatures and Smart Cards," *Proceedings of the 3rd Inernational Smart Card Conference*, Amsterdam, March 1996.

[17] **Chaum** David. *Esprit - Towards a Cashless Society*. Internet WWW page at URL: <http://www.cordis.lu/esprit/src/results/pages/infoind/infind20.htm> (visited April 2001).

[18] **Chaum** David. Achieving electronic privacy. *Scientific American*, Volume 267, No. 2, August 1992. Pages 96-101. [More Results From: http://ganges.cs.tcd.ie/mepeirce/Project/chaum.html] (visited June 2001).

[19] **Chung** Eui-Suk, Dardailler Daniel. *White Paper: Joint Electronic Payment Initiative*, April 9, 1997. Internet WWW page at URL: <http://www.w3.org/ECommerce/white-paper> [More Results From: www.w3.org] (visited May 2001).

[20] **Crawford** Diane. Mediating Electronic Product Catalogs. *Communications of the ACM*, Volume 41, No. 7.

[21] **Creese** Jocelyn, Abric Cecile. The City Card of the Future, *Card Technology Today*, Volume 11, Issue 9, 1 May 2000. Pages 12-13.

[22] **Cummings** L.L., Bromiley P. 1996. The organizational trust inventory (OTI): development and validation", in Kramer R.M. and Tyler T.R. (Eds), *Trust in Organizations: Frontiers of Theory and Research*, Sage Publications, Thousand Oaks, CA. Pages 302-320.

[23] **Dawson** E., Clark A., Looi M. Key management in a non-distributed environment. *Future Generation Computer Systems*, Volume 15, 2000. Pages 319-329.

[24] **Desmarais** Norman. Body language, security and e-commerce. *Library Hi Tech*, Volume 18, No. 1, 2000. Pages 61-74.

[25] **Devargas** M. Survival is Not Compulsory: An Introduction to Business Continuity Planning. *Computers & Security*, Volume, 18, No. 1, 1999. Pages 35-46. Elsevier Science Ltd.

[26] **Docherty** Paul, Simpson Peter. Macro Attacks: What Next After Melissa? *Computers and Security*, Volume 18, No. 5, 1999. Pages 391-395. Elsevier Science Ltd.

[27] **de Vivo** Marco, de Vivo Gabriela O., Koeneke Roberto, Isern Germinal. Internet Vulnerabilities Related to TCP/IP and T/TCP. *Computer Communication Review*, Volume 29, No.1. Pages 81-85.

[28] **Essick** K., Busse T., Guth R. "Ready, SET, Wait". *Info World*, 20(21), May 25, 1998.

[29] **Fellenstein** C., Wood R. 2000. *Exploring E-commerce, Global E-business, and E-societies*. First Edition. Prentice Hall, Inc.

[30] **Ford** R. Malware Briefing. *Computers & Security*, Volume 17, No. 2, 1998. Pages 110-114. Elsevier Science Ltd.

[31] **Franklin** Matthew. 1999. *Financial Cryptography '99 - third international conference*. First Edition. Springer-Verlag.

[32] **Furnell** S. M., Warren M. J. Computer Hacking and Cyber Terrorism: The Reals Threats in the New Millenium? *Computers & Security*, Volume 18, No. 1, 1999. Pages 28-34. Elsevier Science Ltd.

[33] **Furnell** S. M., Karweni T. Security implications of electronic commerce: a survey of consumers and businesses. *Internet Research: Electronic Networking Applications and Policy*, Volume 9, No. 5, 1999. Pages 372-382.

[34] **Garfinkel** Simson L. *How the VirtualPIN works*, Published: Jan. 29, 1996. Internet WWW page at URL: <http://simson.net/clips/96.SJMN.FirstVirtualPIN.html> (visited April 2001).

[35] **Glassman** Steve, Manasse Mark, Abadi Martin, Gauthier Paul, Sobalvarro Patrick. The MilliCent Protocol for Inexpensive Electronic Commerce. *White Papers – Compaq*. Internet WWW page at URL: <http://beta.millicent.digital.com> (visited July 2001).

[36] **Greenstein** Marilyn, Feinman Todd M. 2000. *Electronic Commerce: Security, Risk Management and Control*. First Edition. McGraw-Hill Companies Inc.

[37] **Leebaert** Derek. 1999. *The Future of the Electronic Marketplace*. Second Edition. Massachusetts Institute of Technology.

[38] **Levy** S. Hackers: Heroes of the computer revolution. *Anchor Press / Doubleday.* 1984.

[39] **Handy** C. Trust and the virtual organisation". *Harward Business Review*, Volume 73, No. 3, May-June 1995. Pages 40-50.

[40] **Hawkins** Steve, Yen David C., Chou David C. Awareness and challenges of Internet security. *Information Management & Computer Security*, Volume 8, No. 3, 2000. Pages 131-143.

[41] **Helmstetter** Greg. 1997. *Increasing Hits and Selling More on your Web Site.* First Edition. Wiley.

[42] **Hruska** J. Is the Virus Problem Getting Worse? *Network Security*, Volume 2001, Issue 2, 1 February 2001. Pages 13-16.

[43] **Humphreys** T. Signing the E-word. *Network Security*, Jan 2000. Page 13.

[44] **Isaias** Pedro. *Technology Issues and Electronic Copyright Management Systems*. Internet WWW page at URL: <http://www.ariadne.ac.uk/issue21/ecms/> [More Results From: www.ariadne.ac.uk] (visited February 2001).

[45] **Jajodi** Sushil, Ammann Paul, McCollum Catherine D. Surviving Information Warfare Attacks. *Computer*, Volume 32, No. 4, April 1999. Pages 57-63.

[46] **Jarvis** Neil. E-Commerce and Encryption: Barriers to Growth. *Computers & Security*, Volume 18, No. 5, 1999. Pages 429-431.

[47] **Jayawardhena** Chanaka, Foley Paul. Overcoming Constraints on Electronic Commerce – Internet Payment Systems. *Journal of General Management*, Volume 24, No. 2, Winter 1998. Pages 19-35.

[48] **Keen** Peter, Balance Craig, Chan Sally, Schrump Steve. 2000. *Electronic Commerce Relationships: Trust by Design*. First Edition. Upper Saddle River: Prentice Hall.

[49] **Kendrick** Rupert. Are You Secure? *Computers and Law*, Volume 10, No. 2, June/July 1999. Pages 14-16.

[50] **Kerstetter** J. "E-wallet Eliminates Downloads," *PC Week*, December 21 1998.

[51] **Khiaonarong** T. Electronic payment systems development in Thailand. *International Journal of Information Management*, Volume 20, Issue 1, 2000. Pages 59-72. Elsevier Science Ltd.

[52] **Klur** David. What and Organisation Should Know About Using Electronic Cash. *Information Strategy: The Executive's Journal*, Volume 13, No. 3, Spring 1997. Pages 15-22.

[53] **Kovacichm** G. Electronic-Internet Business and Security. *Computers & Security*, Volume 17, No. 2, 1998. Pages 129-135. Elsevier Science Ltd.

[54] **Krueger** J., Schloss R. (1997). *Facing the Smart Card Security Issue*. Internet WWW page at URL: <http://www.smartcrd.com/info/more/security.htm> (visited November 2000).

[55] **Labuschagne** L., Eloff J.H.P. Electronic commerce: the information-security challenge. *Information Management & Computer Security*, Volume 8, No.3, 2000. Pages 154-157.

[56] **Lambrinoudakis** Costas. Smart card technology for deploying a secure information management framework. *Information Management & Computer Security*, Volume 8, Issue 4, 2000. Pages 173-183. Elsevier Science Ltd.

[57] **Lamond** Keith. *Credit Card Transactions: First Virtual*. Internet WWW page at URL: <http://www.virtualschool.edu/mon/ElectronicProperty/klamond/Fvpymnt.htm> (visited March 2001).

[58] **Lau** O. The Ten Commandments of Security. *Computers & Security*, Volume 17, No. 2, 1998. Pages 119-123. Elsevier Science Ltd.

[59] **Leebaert** Derek. 1999. *The Future of the Electronic Marketplace*. Massachusetts Institute of Technology. Second Edition.

[60] **Leong** Anthony. 1998. *Paper, Plastic, and Now, Electronic*. Internet WWW page at URL: <http://members.aol.com/aleong1631/eps.html> (visited May 2001).

[61] **Levy** S. "E-Money (That's What I Want)," *Wired*, 2(12), December. Page 174.

[62] **Lichtenstein** S. Internet Risks for Companies. *Computers & Security*, Volume 17, No. 2, 1998. Pages 143-150. Elsevier Science Ltd.

[63] **Machlis** Sharon. IBM hedges its bets on SET. *Computers & Security*, Volume 17, Issue 6, 1998. Page 516. Elsevier Science Ltd.

[64] **Maddox** Kate, Blankenhorn Dana. 1998. *Web Commerce. Building a Digital Business.* First Edition. Wiley.

[65] **Marcella** Albert J., Stone Larry, Sampias William J. 1998. *Electronic Commerce: Control Issues for Securing Virtual Enterprises*. First Edition. The Learning Center.

[66] **Marcella** Albert J.R. Controlling The Ethical Use of Information In Electronic Commerce. *EDPACS*, Volume 26, No. 11, March 1999. Pages 1-14.

[67] **May** Paul. 2000. *The Business of Ecommerce: From Corporate Strategy to Technology*. First Edition. Cambridge University Press.

[68] **McDermott** Paul. Building Trust Into Online Business. *Network Security*, Volume 2000, Issue 10, 1 October 2000. Pages 10-12.

[69] **McDonald** Graham. http://www.just.how.risky.is.the.internet? *Management Accounting*, Volume 78, No. 3, March 2000. Pages 74-75.

[70] **Messmer** E. MasterCard, Visa trade strong security for ease of use, *Network World*, Pages 18-19. 22, March 1999.

[71] **Michelson** R., *Rolf's Page on Electronic Payment Systems*. Internet WWW page at URL: <http://www.delab.sintef.no/~rolfm/Security/Payment.html> (visited January 2001).

[72] **Miles** R.E., Snow C.C. 1992. Causes of failure in network organizations. *California Management Review*, Summer. Pages 53-72.

[73] **Mishra** A.K., 1996. Organizational Responses to Crisis – The Centrality of Trust, *Trust in Organizations: Frontiers of Theory and Research*, Sage Publications, Thousand Oaks, CA. Pages 261-287.

[74] **Nelms** C. Internet E-mail Risks and Concerns. *Computers & Security*, Volume 18, No. 5, 1999. Pages 409-418. Elsevier Science Ltd.

[75] **Neumann** Clifford B., Medvinsky Gennady. NetCheque, NetCash, and the Characteristics of Internet. *The Journal of Electronic Publishing*. Volume 2, Issue 1, May 1996. [More Results From: http://www.press.umich.edu/jep/works/NeumNetPay.html] (visited May 2001).

[76] **Nissen** Mark E. The Commerce Model for Electronic Redesign. *Journal of Purchasing*, Volume 1 No. 2, August 1997. [More Results From: Internet WWW page at URL: <http://www.arraydev.com/commerce/jip/9702-01.htm>].

[77] **Nosworthy** J.D. Implementing Security in the 21st Century – Do You Have the Balancing Factors? *Computers & Security*, Volume 19, No. 4, 2000. Pages 337-347. Elsevier Science Ltd.

[78] **O'Daniel Thomas**. 2000. *Electronic commerce. Management economics marketing & technology.* First Edition. Pelanduk Publications.

[79] **O'Mahony** Donald, Peirce Michael, Tewari Hitesh. 1997. *Electronic Payment Systems*. First Edition. ARTECH HOUSE.

[80] **Orr** Bill. PAIN, anyone? The four security pillars of e-commerce, and what they will do for you. *ABA Banking Journal*, Volume 90, No. 10, October 1998. Pages 82, 84, 86.

[81] **Overly** Michael R. 1999. e-*policy*. *How to develop Computer, E-mail, and Internet Guidelines to Protect Your Company and its Assets.* First Edition. AMACOM.

[82] **Pemble** Matthew. Washing Your Laundry in Public – An Analysis of Recent High-Publicity Security Incidents. *Network Security*, Volume 2000, Issue 12, 1 December 2000. Pages 10-12.

[83] **Pfleeger**, C.P. 1997. *Security in Computing*. Second Edition. Upper Saddle River: Prentice Hall.

[84] **Pohlmann** N. Smart Cards: The Authentication Solution for the E-business User. *Network Security*, Volume 2001, Issue 4, 1 April 2001. Pages 12-15.

[85] **Ratnasingham** Pauline. Trust in Web-based electronic commerce security. *Information Management & Computer Security*, Volume 6, No. 4, 1998. Pages 162-166.

[86] **Rayport** J. F. & Sviokla J. H. Managing in the Marketspace. *Harvard Business Review*, November-December 1994. Pages 141-150.

[87] **Rist** O. "Building E-Commerce". *Network Computing Online*, December 1998.

[88] **Rosen** Anita. 2000. *The e-commerce Question and Answer Book.* First Edition. AMACOM.

[89] **Salauen** Anne. E-Commerce. Consumer Protecion – Proposals for improving the protection of online consumers. *Computer Law & Security Report*, Volume 15, No. 3, 1999. Pages 159-157.

[90] **Sarkar** M.B., Butler B., Steinfield C. Intermediaries and Cybermediaries: A Continuing Role for Mediating Players in the Electronic Marketplace. *Journal of Computer-Mediated Communication*, Volume 1, No. 3, 1995. Pages 1-13.

[91] **Sato** S., Humphrey D.B. 1995. *Transforming payment systems: meeting the needs of emerging market economies*. Washington, DC: World Bank Discussion Papers 291.

[92] **Schneider** G.P., Perry J.T. 2000. *Electronic Commerce*. First Edition. Thomson Learning.

[93] **Schwartau** W. 1994. *Information Warfare: Chaos on the Electronic Superhighway*. Thunder's Mouth Press, New York.

[94] **Schwartz** J. Visa, Wells Fargo Pose E-Payment Alternatives. *Internetweek*, 7 June 1999. Pages 1-3.

[95] **Shim** J.K., Qureshi A.A., Siegel J.G., Siegel R.M. 2000. *The International Handbook of Electronic Commerce*. First Edition. AMACOM.

[96] **Sifers** Randall W. *Regulating Money in Small-Value Payment Systems: Telecommunications Law as a Regulatory Model*. Internet WWW page at URL: <http://www.taxi-l.org/emoney.htm> (visited March 2001).

[97] **Sirbu** Marvin A. Credits and debits on the Internet. *IEEE Spectrum*, Volume 34, Issue 2, February 1997. Pages 23-29.

[98] **Timmers** Paul. 1999. *Electronic Commerce Strategies and Models for Business-To-Business Trading*. Second Edition. Wiley.

[99] **Tison-Dualan** Loida, Gallegos Frederick. Electronic Funds Transfer: Control Issues in a Cashless, Checkless Society. *EDPACS*, Volume 27, No. 9, March 2000. Pages 8-14.

[100] **Verschuren** T. "Smart access: strong authentication on the web". *Computer Networks and ISDN Systems*, 1998, Volume 30. Pages 1511-1519.

[101] **von Solms** Rossouw. Information security management (1): why information security is so important. *Information Management & Computer Security*, Volume 6, No. 4, 1998. Pages 174-177.

[102] **Wagner** Mitch. Online security a pipe dream? *Computers & Security*, Volume 15, Issue 2, 1996. Page 125.

[103] **Webb** Steve. Crimes and Misdemeanours: How to Protect Corporate Information in the Internet Age. *Computers & Security*, 2000, Volume 19, No. 2. Pages 128-132.

[104] **Weinberg**, Neal. Digital dough fails to rise. *Network World*, April 12, 1999.

[105] **Westland** Christopher J., Clark Theodore H.K. 1999. *Global Electronic Commerce. Theory and Case Studies.* First Edition. Massachusetts Institute of Technology.

[106] **Whinston** Andrew B., Choi Soon-Yong. Smart Cards. Enabling Smart Commerce in the Digital Age. *CREC/KPMG White Paper*, May 1998. Internet WWW page at URL: <http://cism.bus.utexas.edu/works/articles/smartcardswp.html> (visited May 2001).

[107] **Williams** Deryck. On good authority. Digital Certificates. *CA Magazine*, Volume 132, No. 9, November 1999. Pages 43-44.

[108] **Winfield** Tresse G., Lawrence C. Stewart. 1998. *Designing Systems for Internet Commerce*. First Edition. Addison Wesley.

[109] **You** Chen-Hwee, Zhou Jianying, Lam Kwok-Yan. On the Efficient Implementation of Fair Non-repudiation. *Computer Communication Review*, Volume 28, No. 5, October 1998. Pages 50-60.

[110] **Zhou** J., Lamb K.Y. Securing digital signatures for non-repudiation. *Computer Communications*, Volume 22, No. 8, 25 May 1999. Pages 710-716.

[111] **Zuckerman** Gregory. "Borrowing Levels Reach a Record, Sparking Debate". *The Wall Street Journal*, July 5, 2000.

[112] Answers to Frequently Asked Questions. About Smart Cards. Internet WWW page at URL: <http://www.smartcardforum.org/info/whatis/faq.htm> (visited April 2001).

[113] *ARPANET to Internet and the Protocol that lead to Growth*. Internet WWW page at URL: <http://www.patkinson.cwc.net/ind1a.htm> (visited January 2001).

[114] *ARPANET Internet: Atlas of Cyberspace 05/08/00*. Internet WWW page at URL: <http://www.geog.ucl.ac.uk/casa/martin/atlas/historical.html> (visited December 2000).

[115] Card Europe UK (1996). *Smart Card Technology Background Paper*. Internet WWW page at URL: <http://www.gold.net/users/ct96/rep1.htm> (visited September 2000).

[116] CIO. "First cyber terrorist action reported". *The magazine for information executives*. Volume 3, No. 2, March 2001. Associated Press. 1998. May 6th, USA.

[117] *Commerce on the World Wide Web*. Internet WWW page at URL: <http://ei.cs.vt.edu/~jwww/courseNotes/security/commerce.html> [More Results From: ei.cs.vt.edu] (visited March 2001).

[118] Comparing IQs. *Enterprise Technologies*. July 2000. Internet WWW page at URL: <http://www.avcom.com/et/online/> (visited February 2001)

[119] *CyberCash Secure Credit Card*. Internet WWW page at URL: <http://www.infoboard.com/IB1/mn_ccash.html> [More Results From: www.infoboard.com] (visited April 2001).

[120] *CyberCash home page*. Internet WWW page at URL: <http://www.cybercash.com> (visited April 2001).

[121] *CyberCoin home page*. Internet WWW page at URL: <http://www.cybercash.com/cybercash/services/cybercoin.html> (visited April 2001).

[122] DigiCash files Chapter 11. *Tech News – CNET.com*, November 4, 1998. Internet WWW page at URL: <http://new.cnet.com/news/0,10000,0-1003-200-334992,00.html> (visited July 2001).

[123] *Digital Money Online*. Internet WWW page at URL: <http://www.intertrader.com/library/DigitalMoneyOnline/dmo/dmo_c.htm> (visited April 2001).

[124] *Ecash (DigiCash) Homepage*. Internet WW page at URL: <http://www.digicash.com> (visited April 2001).

[125] *eCheck (FSTC Electronic Check) Homepage*. Internet WWW page at URL: <http://www.echeck.org> (visited April 2001).

[126] *Electronic Payment Systems*. Internet WWW page at URL: <http://www.isi.edu/people/bcn/tutorials/sndss98/isocep/ppframe.htm> [More Results From: www.isi.edu] (visited May 2001).

[127] *Electronic Payment Systems for Selling Entertainmnet Events on the World Wide Web*. Internet WWW page at URL: <http://www-scf.usc.edu/~backe> (visited September 2000).

[128] *Encyclopedia listing for IT terms*. Internet WWW page at URL: <http://www.whatis.com> (visited 2001)

[129] eVerlage. Internet WWW page at URL: <http://medoc.informatik.tu-muenchen.de/Chablis/MStudy/4_14_CyberCoin.html> [More Results From: medoc.informatik.tu-muenchen.de] (visited July 2001).

[130] Financial Service Technology Consortium, *Electronic Payments Infrastructure: Design Considerations*, 1995. Internet WWW page at URL: <http://www.fstc.org/projects/commerce/public/epaydes.htm> (visited February 2001).

[131] *Financial Services Technology Consortium*. Internet WWW page at URL: <http://www.fstc.org/> (visited February 2001).

[132] *First Virtual website*. Internet WWW page at URL: <http://www.fv.com> (visited April 2001).

[133] *FNC Resolution: "Definition of "Internet"*. October 24, 1995. Internet WWW page at URL: <http://www.fnc.gov/Internet_res.html> (visited June 2000).

[134] *Frequently asked questions by the Press - Tim BL*. Internet WWW page at URL: <http://www.w3.org/People/Berners-Lee/FAQ.html> (visited January 2001).

[135] *GlobeSmart Electronic Wallet Solutions*. Internet WWW page at URL: <http://www.globesmart.com/solutions/gs_ss_wallet.htm> (visited April 2000).

[136] Group 5 - *Secure Electronic Payment Systems*. Internet WWW page at URL: <http://ecommerce.vanderbilt.edu/Student.Projects/secure.payment.systems/overview.html> (visited May 2001).

[137] *History of Electronic Cash Menu*. Internet WWW page at URL: <http://www2.darden.edu/case/cybercash/menu/history.htm> (visited February 2001).

[138] *IASIW. Information Warfare, I-War, IW, C4I, Cyberwar*. Internet WWW page at URL: <http://www.psycom.net/iwar.1.html> (visited June 2001).

[139] *IMC Online - E-Commerce – CyberCash*. Internet WWW page at URL: <http://imconline.com/main/main_ecommerce_cyber.htm> [More Results From: imconline.com] (visited April 2001).

[140] *InstaBuy home page*. Internet WWW page at URL: <http://www.instabuy.com/> (visited June 2001).

[141] *InterIntermediaries: New places for producing and manipulating web content*. Internet WWW page at URL: <http://www.almaden.ibm.com> (visited April 2001).

[142] *MilliCent home page*. Internet WWW page at URL: <http://www.millicent.digital.com/> (visited May 2001).

[143] *Mondex home page*. Internet WWW page at URL: <http://www.mondex.com> (visited May 2001).

[144] *NetBank home page*. Internet WWW page at URL: <http://www.netbank.com/~netcash> (visited January 2001).

[145] *NetBill*, Carnegie Mellon University. Internet WWW page at URL: <http://www.ini.cmu.edu/netbill/> (visited May 2001).

[146] *Net Business, a collection of case studies in e-commerce*. Internet WWW page at URL: <http://www.techweb.com/netbiz> (visited 2001)

[147] *NetCash home page*. Internet WWW page at URL: <http://nii-server.isi.edu/info/netcash/> (visited January 2001).

[148] *NetCheque network payment system*. Internet WWW page at URL: <http://www.isi.edu/gost/info/NetCheque/> (visited April 2001).

[149] *NetChex website*. Internet WWW page at URL: <http://www.netchex.com/index.html> (visited April 2001).

[150] *Netscape Inc., SSL Protocol*. Internet WWW page at URL: <http://home.netscape.com/newsref/std/SSL.html> (visited January 2001).

[151] *PGP, The International PGP Home Page*. Internet WWW page at URL: <http://www.pgpi.com/> (visited January 2001).

[152] *Product: Smart-Bank : The electronic wallet*. Internet WWW page at URL: <http://www.ilink.co.uk/p_smbk2.html> (visited April 2000).

[153] *RSA Security Hompage: Detailed FAQ on S-MIME*. Internet WWW page at URL: <http://www.rsasecurity.com/standards/smime/faq.html> (visited July 2001).

[154] *Secure Electronic Transactions (SET) - MasterCard*. Internet WWW page at URL: <http://www.mastercard.com/shoponline/set/set.html> [More Results From: www.mastercard.com] (visited May 2001).

[155] *Smart Cards: A Draft*. Internet WWW page at URL: <http://www.cous.uvic.ca/poli/bennett/courses/456/fm/messages/18.htm> (visited April 2001).

[156] *Smart Cards & Electronic Payment Systems*. Internet WWW page at URL: <http://www.knowthis.com/ecommerce/smartcards.htm> (visited May 2001).

[157] Smart cards set to maintain 20%-25% growth, *Card Technology Today*, Volume 12, Issue 4, 30 November 2000. Page 2.

[158] *State of the art in e-business*. Internet WWW page at URL: <http://www.telin.nl/dscgi/ds.py/Get/File-3731/State_of_the_art_in_e-business_services_and_components.pdf> (visited August 2001).

[159] *Summary of Electronic Payment Systems (EPSs)*. Internet WWW page at URL: <http://www.backe.com/epssum.html> (visited April 2001).

[160] *SURFnet Public Key Infrastructure – Inleiding Public Key Infrastructure*. Internet WWW page at URL: <http://pki.surfnet.nl/inleiding_PKI.php> (visited July 2001).

[161] *Telecom Glossary 2000*. Internet WWW page at URL: <http:\\www.its.bldrdoc.gov> (visited January 2001).

[162] The Federal Reserve Bank of Minneapolis. *The History of Money*. Internet WWW page at URL: <http://woodrow.mpls.frb.fed.us/econed/curric/history.html> (visited January 2001).

[163] *The Journal of Electronic Publishing* [Online], Volume 2, Issue 1, May 1996. ISSN 1080-2711. Internet WWW page at URL: <http://www.press.umich.edu/jep/works/NeumNetPay.html>

[164] The smart card market in 2001, *Card Technology Today*, Volume 2001, Issue 2, February 2001. Pages 13-14.

[165] The smart card industry at last comes of age, *Card Technology Today*, Volume 2001, Issue 1, 31. January 2001. Pages 10-13.

[166] *The Three Layer Model – Computer and human Intermediaries*. Internet WWW page at URL: <http://www.hermans.org/agents/h42.htm> (visited April 2001).

[167] *Transaction Net: Check or Credit / Debit Card Payments*. Internet WWW page at URL: <http://www.transaction.net/payment/3party.html> [More Results From: www.transaction.net] (visited July 2001).

[168] *Vertical Marketspaces. Issue #2*. Internet WWW page at URL: <http://www.vtopia.com/resources/ebusinss/issue2.html> (visited April 2001).

[169] *Webopedia Definition and Links*. Internet WWW page at URL: <http://webopedia.internet.com> (visited February 2001).

[170] *ZDNet – News on electronic commerce*. Internet WWW page at URL: <http://www.zdnet.com/enterprise/e-business> (visited 2001).

Index of Acronyms

Glossary

♦ A

Access control

Access control restricts the use of a resource to only those users that have the correct authorisation. The term therefore, implies the prevention of unauthorised use of a resource.

Acquirer

The acquirer in an electronic money system is the financial institution that holds deposit accounts for merchants and to which transaction data are transmitted.

Algorithm

A set of rules that specify a method of carrying out a task (e.g. encryption algorithm).

American National Standards Institute (ANSI)

The ANSI sets and approves standards and represents and co-ordinates U.S. interest in international non-treaty and non-government standards bodies.

Anti-virus software

An anti-virus software program can help scan and subsequently detect viruses.

ARPANET

APRANET, which stands for Advanced Research Projects Agency Network was the first Internet. The U.S. Department of Defense developed the APRANET as an experiment in wide-area-networking in order to survive a nuclear war. Compared to the Internet, the ARPANET was a closed network, operating between fixed locations, while the Internet is available on a global scale.

Audit trail

A sequential record of events that occurred in a system.

♦ B

B2B (Business-to-Business) marketspace

This kind of marketspace involves one business enterprise selling to another.

B2C (Business-to-Consumer) marketspace

The term B2C is commonly used to refer to the sale by a business enterprise to a person (or consumer). The term is misleading, in that a business enterprise may also be a consumer.

Backbones

High-speed lines or series of connections that form major pathways within the telecommunications networks.

Bank Internet Payment System (BIPS)

The BIPS project provides a specification for a protocol and secure server for banks to provide payment transactions services over the Internet by developing several components that are necessary to support secure electronic transactions. It therefore, focuses on encouraging companies - and eventually consumers - to process a variety of electronic payment transactions via the Internet.

Blind signatures

Blind signatures allow a document to be signed without revealing its contents. Using such signatures, protocols for secure distributed electronic banking and secure online voting can be designed. The DigiCash system delivers e-cash from a financial institution without revealing the name of the person authorising the delivery.

Bob Kahn

Co-designer of TCP/IP.

Browser

A client program (software) used to "look" (browse) at various kinds of Internet resources. Examples are, Netscape Navigator and Microsoft Explorer.

◆ C

C2C (Consumer-to-Consumer) marketspace

C2C is an often over-looked category of marketspaces, which supports transactions between individuals. Examples of these are "classified ads" and auctions of personal possessions. Others involve "indirect or deferred reciprocity". Still others involve gifts.

Certificate

Depending on the public key infrastructure implementation, the certificate includes the owner's public key, the identity of an entity, the expiration date of the certificate, and other information about the public key owner, digitally signed with the private key of the issuing certification authority. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

Certification Authority (CA)

A CA is an authority in a network that issues, manages and signs security certificates. These security certificates are mostly used in SSL connections.

Channel

A unidirectional route for communication, which forms a permanent route to a group of customers.

Client

A program that accesses services from another computer called the server.

Cryptoanalysis

The area of cryptography dedicated to studying and developing methods by which, plaintext may be deduced from the ciphertext.

♦ D

DARPA (Defense Advanced Research Projects Agency)

The research organisation that funded the ARPANET.

Data Encryption Standard (DES)

DES is an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard. DES is a symmetric cryptosystem: when used for communication, both sender and receiver must know the same secret key.

Diffie-Hellman

The Diffie-Hellman key agreement protocol was developed in 1976 by Diffie and Hellman. The protocol allows two users to exchange a secret key over an insecure medium, without any prior secrets.

Digest

A value computed from a data set, which can be thought of as a digital signature that can be checked to ensure that the data set has not been altered since the original creation.

Digital Signature Algorithm (DSA)

An asymmetric cryptographic algorithm that generates a digital signature for the authentication of electronic documents in the form of a pair of large numbers. The signature is computed according to the specified algorithm within parameters such that

the identity of the signer and the integrity of the signed data can be verified. This algorithm uses a private key to sign a message and a public key to verify the signature.

♦ E

Electronic catalogues

The means to electronically access a listing of goods and services available for purchase.

Electronic Commerce Modelling Language (ECML)

ECML is an open specification for exchanging information of payments.

Electronic Data Interchange (EDI)

EDI is the automated exchange of business information (such as, purchasing orders, invoices etc.) among computers of different business entities in a standard format, across dedicated communications networks.

Electronic Funds Transfer (EFT)

EFT is a mechanism facilitating electronic payments, such as, direct deposits of salaries into the bank accounts of workers. EFT is therefore, used between accounts at point of sale (POS) and is sometimes referred to as EFTPOS (Electronic Funds Transfer at the point of sale).

El Gamal Algorithm

An algorithm for symmetric cryptography invented in 1985 by Taher El Gamal that is based on the difficulty of calculating discrete logarithms and can be used for both encryption and digital signatures.

Electronic mail (E-mail)

Electronic mail refers to messages, usually text, sent from one person to another via computer. In 1972, the first electronic mail delivery involving two machines was arranged by Ray Tomlinson at BNN (Bolt, Beranek & Newman, originally an acoustics

consulting firm founded in 1948). The program was written in two parts, SNDMSG was used to send messages, READMAIL to receive them.

E-mail bomb

A mail bomb is the sending of a massive amount of e-mail to a specific person or system. This huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop functioning. In the past, mail bombs have been used to "punish" Internet users who have been violators of netiquette (for example, people using e-mail for undesired advertising, or spam).

E-mail spam

The online equivalent of junk mail is referred to as spam mail. Spam mail is flooding the e-mail boxes with mails (mostly related to advertisements). As the visitor or customer does not request these mails they are viewed negatively by the public.

E-mail spoofing

E-mail spoofing occurs when a perpetrator, pretends he is somebody else, by changing his identity in an e-mail packages. In this way the recipient of the e-mail thinks the sender (in this case the perpetrator) is someone else. E-mail spoofing can be prevented using digital signatures.

Embedding

In integrated circuit manufacturing, the process by which the chip module is mounted on the plastic card.

Exhaustive attack

A *trial-and-error* attempt to violate computer security by systematically attempting to use a very large number of possible passwords or keys.

Extranet

The extranet, is a network outside of, but connected into, the companies network segments. It can be seen as a bridge between the public Internet and private Intranets (see Intranet), which allows connection of multiple companies behind firewalls. In a sense, the extranet is providing an exterior security boundary that protects the organisations from the open network, while providing lower security boundaries for greater sharing of information between the partners.

♦ F

Fast Encipherment Algorithm (FEAL)

FEAL is a block cipher developed as an alternative to DES by Shimizu and Miyaguci.

File Transfer Protocol (FTP)

FTP is a protocol used to transfer files from one computer to another over the Internet. It is most commonly used to upload files or web documents to a server.

Financial Services Technology Consortium (FSTC)

FSCT is comprised of about 100 members including major banks, financial service providers, national laboratories, universities and government agencies sponsoring and participating in collaborative research and development on technical projects.

♦ G

Gateway

A gateway represents a hardware and software set-up that translates between networks using two dissimilar protocols. Therefore, it is a mechanism for providing access to another system.

♦ H

Hoax

A false virus warning – usually an e-mail mailed in chain letter fashion describing a highly unlikely dangerous type of virus.

HyperText Markup Language (HTML)

The HTML is sometimes referred to as the offspring of SGML. It is a simple programming language used for writing pages for the World Wide Web. The code begins and ends with <HTML> and </HTML> respectively and it is divided into a header and body section.

HyperText Transfer Protocol (HTTP)

HTTP is the underlying protocol used by the World Wide Web (WWW), and allows communications between linked computers all over the world. HTTP defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands. When a user enters a Uniform Resource Locator (URL) in a browser, he/she is sending an HTTP command to the web server directing it to retrieve and transmit the requested document.

♦ I

Information

Organised data, which is understood to have significance and meaning.

Information Highway

The Information Highway is a rapid transit system of bulletin board services, online services, and other services that enable people to obtain information from telecommunications networks.

Institute of Electrical and Electronics Engineers (IEEE)

The IEEE is a scientific, engineering and educational society that develops and publishes standards in a variety of electrical engineering and computer-related areas.

Integrated Circuit Card (Chip Card)

A plastic card in which one or more integrated circuits are embedded.

Interface Message Processor (IMP)

The ARPANET network interface.

International Data Encryption Standard (IDEA)

IDEA is a block cipher that operates on 64-bit plaintext blocks. The same algorithm is used for both encryption and decryption.

International Standards Organization (ISO)

The ISO was founded in 1947 with the aim of reaching international agreements on standards. It is a world-wide federation of national standard bodies from over 120 member countries.

Internet Service Providers (ISPs)

ISPs establish permanent connections into the Internet and then rent this connection to smaller users on an ad hoc (or dial-up) basis.

Intranet

Any private network utilising Internet technologies to enable users to communicate and access information within an organisation's boundaries. Intranet users can access the Internet, but firewalls keep outsiders from accessing confidential data.

Issuer

The issuer in an electronic money system is the entity, which receives payment in exchange for value distributed in the system.

♦ K

Kerberos

Kerberos is an authentication system developed at the Massachusetts Institute of Technology (MIT). It provides authentication using conventional cryptography, i.e. shared secret key in order to enable two parties to exchange private information across an otherwise open network. A unique key, called a *ticket*, is assigned to each user that logs to the network. The ticket is then embedded in messages in order to assure that the user is who they claim to be.

Key management

The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

♦ L

Lawrence Roberts

The ARPANET Program Manager.

Leonard Kleinrock

The pioneer of digital network communications who helped to built the first ARPANET.

Local Area Network (LAN)

The LAN is a network linking terminals, programs and storage at multiple work sites, over a small geographic area.

♦ M

Marketplace

A marketplace is the physical channel to a market. The concept of "marketspace" is used to distinguish the "location" in which electronic commerce is conducted from conventional physical marketplaces.

Message Digest

Fixed length code appended to a message, which serves as integrity check for a message. A message digest can be implemented with the help of hash-functions.

Micro-payments

Payments of small amounts are called micro-payments.

Mosaic

The first WWW browser that was available and which really started the popularity of the Web.

Multipurpose Internet Mail Extensions (MIME)

MIME is the specification for formatting non-text (non-ASCII) messages so that they can be sent over the Internet. Non-text files include graphics, spreadsheets, formatted word-processor documents, sound files etc. A new version, called S/MIME, supports encrypted messages.

♦ N

Net

Net is an abbreviation for the term Internet.

Network

A collection of two or more linked computers, which can exchange data, share resources and make use of each other's software. Networks allow people to communicate. They are classified as Local Area Networks (LAN) and Wide Area Networks (WAN).

Network Control Program (NCP)

The first Internet network protocol.

Network Spoofing

In network spoofing a system presents itself to the network as though it was a different system. This is a common method used by hackers to gain access to a system.

NSFNet

The National Science Foundation's Network.

♦ O

Offline

When no direct connection is made between devices, involved in a transaction in an electronic payment system, and the centralised computer system the transaction is called offline.

Online

When a transaction is online, a direct connection between the devices, involved in a transaction in an electronic payment system, and the centralised computer system exists.

Open network

A telecommunications network that has no access restrictions.

♦ P

Packet-switching

A method of fragmenting messages into sub-parts called packets (which can routed separately), routing them to their destinations in the most efficient way and reassembling them at the destination.

Password

A code used to gain access to protected networks, systems or files.

Personal Identification Number (PIN)

A PIN is a sequence of digits used to verify the identity of a device holder.

Portal

A portal is a Web site that provides a branded "port of entry" to an array of resources and services on the Internet. Portals link companies, customers and business partners, providing them with the information or Web application they need instantly. Companies deploy business portals in order to handle the large number of users and applications that are supported on the Web.

Protocol

A protocol is an agreed method of communication and transmitting data between any telecommunication devices (i.e. regardless of the platform(s) involved).

Public-key Infrastructure (PKI)

A public-key infrastructure is a horizontal structure of CAs, which are subjected to the same organisational, technical and procedural rules and which may (cross-) certify each other. This infrastructure is needed for trustworthy distribution of public keys.

♦ R

RC5

RC5 is a block cipher developed by Rivest for RSA Data Security.

Repudiation

The denial by one of the parties involved in a transaction or communication of having participated in all or part of the transaction or communication.

Revoke a certificate

To make a certificate permanently ineffective from a specified time forward.

Risk Management

Risk management is a methodology that tries to balance the negative consequences potential risk against the cost of implementing associated prevention and detection devices.

Rivest-Sharmir-Adelman (RSA)

RSA, invented in 1977, is a public-key cryptosystem, named after its investors Rivest-Shamir-Adelman. RSA is the encryption used by Netscape in the SSL protocol.

♦ S

Security Policy

The set of rules set down by the security authority governing the use and provision of security services and facilities.

Server

A computer that provides a service to other computers on a network. A server houses the Web sites.

Service Provider

A service provider is a company who supplies Internet services to personal users or businesses.

Sniffing

To capture the information going over the network is called sniffing.

Spoofing

The interception, alteration and retransmission of data in such a way as to mislead the receiver.

Standard Generalized Markup Language (SGML)

SGML is a data encoding system used for organising and tagging elements in a document to enable the electronic exchange of documents between dissimilar systems. The information in SGML documents is divided into data, structure and format.

Suspend a certificate

To make a certificate temporarily ineffective for a specified time.

♦ T

Time-stamping service

A time-stamping service creates time-stamps, which associate a date and time with a digital document in a cryptographically strong way. Non-repudiation services require trust in the time a message was issued or when a certificate was valid and use time-stamps for this purpose.

Time stamps

Time stamps are used to indicate the time that a particular event or action took place, for example, whether an electronic document was created or signed at (or before) a certain time. Digital time stamping is an important non-repudiation technique.

Token

A string of digits representing an amount of a particular currency. If tokens exist, each token is digitally stamped by a bank for authentication purposes.

Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP is the protocol suite that drives the Internet, i.e. Internet network protocol. This protocol suite handles network communications between network nodes (for example computers). The IP handles moving packets of data between host computers. It forwards each packet based on an IP address. The TCP is responsible for verifying the correct delivery of data from client to server. Data can potentially be lost in the intermediate network, and TCP adds support to detect errors or lost data. It will trigger retransmission until the data is correctly and completely received.

Tripel-DES

Tripel-DES is a variation of DES; it encrypts a grouping of data or plaintext three times, each time with a different key. It will encrypt a 64-bit block, using key A, followed by decrypting the result with key B, and then encrypt the result with key C.

Trusted time-stamping authority (TSA)

A time-stamping authority is a trusted third party that provides a time-stamping service. A time-stamping authority may be used for example, by another trusted third party to verify that a digital signature was applied to a message before the corresponding certificate was revoked. This would then allow a revoked public-key certificate to be used again for the verification of a signature created prior to the time of revocation.

◆ U

Uniform Resource Locator (URL)

A URL is the global address of documents and other resources on the WWW. The first part of the address (i.e. http://) indicates what protocol to use. The second part specifies the IP address (i.e. http://www.becrc.org) that identifies the unique server assigned to the domain name. The final part tells the server where the document or resource is located on the server (i.e. http://www.becrc.og/http.htm).

◆ V

Vinton Cerf

Co-designer of TCP/IP.

Virtual Private Network (VPN)

Refers to a network in which some of the parts are connected using the public Internet, but the data sent across the Internet is encrypted, so the entire network is "virtually" private. It is virtually private as the encryption takes place on the originators own private network and the decryption takes place on the recipient's private network.

◆ W

Wallets

Many electronic payment systems use an electronic wallet - a piece of software that a customer can use to store his electronic credit cards, cash, or both. Usually, the wallet also stores personal data and preferences.

Web

An abbreviated term for the World Wide Web.

Wide Area Network (WAN)

WAN is a network typically spanning large geographic areas.

World Wide Web (WWW)

The World Wide Web Internet system uses browsers to handle data and provides full text and graphical access to documents, which have been created using Hypertext Markup Language (HTML).

World Wide Web Consortium (W3C)

W3C is an international industry consortium, founded in 1994, by Tim Berners-Lee. The organisation's purpose is to develop open standards to lead the Web to its full potential as a forum for information, e-commerce, communication, and collective understanding. The W3C is the chief standards body for HTTP and HTML.

X.509

X.509 is an ISO standard for digital certificates. Both Netscape and Microsoft use X.509 certificates to implement SSL in their Web servers and browsers.