TECHNICAL REPORT

DEPARTMENT OF COMPUTER SCIENCE

DIGITAL CASH: ELECTRONIC COMMERCE OVER OPEN NETWORKS

Report No 325

Feb 1999

Digital Cash: Electronic Commerce Over Open Networks

James Mankin and James Malcolm

This technical report was originally a BSc project submitted in April 1997

Student: James Mankin

Supervised by: James A Malcolm

Department of Computer Science

CONTENTS

INDEX OF FIGURES

INDEX OF TABLES

ABSTRACT

The unparalleled success of the Internet has led to much debate about its inability to securely handle financial transactions. Electronic Data Interchange (EDI) is currently the de facto standard for the exchange of trade data, but the interest in the Internet amongst private users and business has made this a potentially very powerful and perhaps lucrative medium for conducting commerce. However, there is no widely adopted payment system that fulfils the needs of all interested parties.

This report looks into electronic commerce and evaluates payment systems that are being developed for open networks, mostly focusing on the Internet.

This report identifies key requirements that successful use of the Internet must impose on payment mechanisms. The payment systems can be classified as token, credit/debit or cash-based systems, examples of which are DigiCash, CyberCash and Mondex. Each system is evaluated in-depth against a general set of requirements which include security, global acceptance and ease of use and also against 3 hypothetical scenarios to obtain system strengths and weaknesses. DigiCash is best but this is attributed to omissions in functionality and use by the competing systems rather than the strength of the DigiCash system itself.

The text highlights the ways in which electronic commerce can be used and illustrates what the features of the main systems are. For this reason it should be read by researchers and I.T. enthusiasts interested in the implications and expectations of this area and also by merchants looking to experiment with selling goods and services over open networks. The report systematically shows, for example, why a merchant should choose one system over another.

The conclusion to this report details improvements that need to be made to allow electronic commerce to flourish. A major issue is the inability of Internet protocols to offer service guarantees. Other issues include the need to have open standards to allow interoperability and the need for future software to embrace future needs such as interactive product specifications.

ACKNOWLEDGEMENTS

I would like to take this opportunity to acknowledge the support that I received from my project supervisor, James Malcolm. His guidance, as well as general enthusiasm and encouragement was much appreciated.

I am also grateful to Jasper Toxepus at DigiCash and Lindsey Read at Mondex for helping me to understand the intricacies of their respective products.

Finally, I would like to thank Vanessa Reynolds who has gracefully listened to my constant ramblings about smart cards and payment mechanisms.

CHAPTER ONE

INTRODUCTION

1.1 INTRODUCTION

The aim of this project is to discuss theories and technical issues concerning on-line electronic cash and then to apply the knowledge gained from this to everyday experiences, gauging the benefits of each mechanism to a particular situation.

1.2 PROJECT MOTIVATION

This Final Year Project was motivated by a desire to understand the unification of Information Technology and Banking. My initial choice of project was to take an in-depth look into the Electronic Funds Transfer (EFT) system that carries trillions of Pounds and Dollars around the world in inter-bank transfers every day. However this is a well developed and mature system and therefore does not lend itself well to being studied in depth. As the network is also private, information about it is much comparatively hard to obtain.

During my initial project evaluation process, I encountered many references to names such as 'CyberCash' and 'DigiCash', and my inquisitive urges insisted that I take a look.

This is how I came to stumble upon this particular facet of electronic commerce. In contrast to the inter-bank clearing network which is a closed system, the Internet supports an open architecture, has over twenty million regular users world-wide and experiences a high growth rate.

The network was originally designed for the use of the military and academics, although research from 1994 [MOO] suggests that at the time 30-35% of European Internet hosts were of a commercial basis. From this figure, I deduced that the level of activity of commercial companies on the Internet must eventually cause a shift at some stage towards the adoption of electronic money. The field of electronic commerce would no doubt have to adapt to a period of rapid change.

My theory is now that the commercial realities of the convergence between banking and telecommunications will drive electronic commerce forward. Why? Because:

- Banks will gain from the ability to provide a wide range of services over new channels, the ability to interact with the customer after normal banking hours and the reduction in cash handling charges.

- Retailers can also benefit from reduced cash handling charges and 24-hour 'shop-windows'.

- Users can benefit from an alternative to cash with no transaction fees, the ability to shop in unsociable hours and the ability to buy goods and services (almost) anonymously.

Therefore I decided to investigate the concepts and key mechanisms available in the very new area of Internet commerce.

1.3 AIMS AND OBJECTIVES

My overall aim as defined in my project objectives is to deliver a paper detailing the current and future prospects of electronic commerce and to comment on what a successful electronic commerce solution should entail. I propose to complete the research in an effective and efficient way.

It is also my intention to gain knowledge and experience in areas of network security and financial analysis. It is important for me to utilise my experience of project management, building on my Industrial Placement year as a Systems Analyst and Project Manager at the European Research and Engineering Centre of Ford Motor Company. This is of course secondary to the process of project work.

The objectives for this project were defined very near to the deadline, due to the time it took to decide not to further investigate the Inter-Bank Funds Transfer system. With no knowledge of electronic commerce, I decided that my aims should therefore be relatively stringent, to provide me with a strict direction to head in.

My core objectives stated at the beginning of the project were:

- Understand Electronic Commerce as a concept well enough to identify key functions of a system and to model particular mechanisms.
- Identify the key requirements of a successful payment mechanism based on a full understanding of currently available systems.
- Evaluate mechanisms available against requirements assigned. Subject the results to real life paradigm comparison to learn core competencies.
- What makes a good system? Which mechanisms serve a particular purpose well? What is the direction of electronic commerce? Is it viable?

It can be seen that I have endeavoured to evaluate electronic commerce from start to finish. There can be no doubt that it is a particularly wide area of study, although as there are no standards currently in place, it goes to focus the fact that we need to look at all the possible available systems.

My advanced objective defined at the beginning of the project was:

- Implement an electronic payment system to serve pieces of information to a community. Verify various factors of the mechanism such as the software, the ease of use and others.

At the time of writing this could not be detailed further, as the strength of arguments presented from my core objectives would no doubt have an impact on the type of software implemented.

My key word for this project is: EVALUATE. As a research project the main aim is to extend the knowledge that is available and to provide insight into that which I study.

1.4 READERSHIP

This report describes the process by which I carried out the project. The technical matter is mostly based around networking, with issues ranging from internetworking to in-depth security.

This text is primarily aimed at students and the research community who have knowledge of all general aspects of computing, with an underlying understanding of mathematics and commerce. It will also be of interest to merchants looking into selling products on he Internet. Explanations will be given for the use of advanced material, although I have tried to structure the text so that it is readable by anybody.

1.5 REPORT STRUCTURE

This project has been organised into chapters which should illustrate a logical development of the research and problem solving process. Each chapter demonstrates a section of the project significant to its overall completion. The chapter size is not indicative or proportional to the amount of time allocated to that aspect of project work. This can be determined by the scheduling of activities given in Chapter 13 (Project Management). The following gives an overview of each chapter. It should be noted that Chapters 2 to 12 represent the 'deliverable' part of the project.

Chapter Two - Background Information. Associated background information of this project is explained including explanations of the growth of the Internet and the function of money. Included are future trends regarding E-cash and factors that influence the growth of electronic commerce.

Chapter Three - Electronic Payment Models. This chapter contains the results of research into payment models on to which an Internet payment method could be mapped. The three models tie in very closely to existing physical payment methods.

Chapter Four - Security. Arguably the most important feature when discussing Internet transactions of any kind, this chapter looks at some of the security mechanisms that can be employed by electronic payment mechanisms. The security methods range from simple hash functions to complex cryptographic algorithms.

Chapter Five - Payment Systems. This chapter contains an evaluation of payment systems that currently support on-line electronic commerce. The chapter divides the systems into the three models found in Chapter 3.

Chapter Six - Payment System Requirements. This chapter deals with what should form the basis of an electronic payment system and aims to map out the key requirements that a user needs. The requirements are divided into three distinct categories - security requirements and commercial requirements, while constraints are also an important issue.

Chapter Seven - Mechanisms Versus Requirements. By looking at what each payment mechanism offers in relation to the requirements listed in Chapter 6, it may be slightly easier to conclude on what makes a good payment system.

Chapter Eight - CyberCash. This is an in-depth study of the CyberCash system. It represents the credit/debit based model discussed in Chapter 3 and includes details about the formatting of messages, the components of the system and an evaluation.

Chapter Nine - Mondex. The chapter studies Mondex as an example of a 'cash' based model. By looking at how it works and its security model it is possible to gain an understanding of a subject with which there is no major academical study.

Chapter Ten - DigiCash. This is the third representative of the models discussed in Chapter 3. Security and authentication form a distinct part of the insight in to this token based payment system.

Chapter Eleven - Putting the Systems into Practice. By using three situations to assess the mechanisms the chapter looks at concluding which payment mechanism will make an ideal electronic payment system.

Chapter Twelve - Trends in Electronic Commerce. This chapter provides an insight into the trends that can be expected to be seen emerging in the field of electronic commerce that are concluded from this study.

Chapter Thirteen - Evaluation. Chapter 13 concludes the project by assessing and evaluating the work that was done and how closely it aligned to the objectives that were stated. It also gives an insight into the problems that were encountered and how the project was managed.

A bibliography and a glossary are included to aid the understanding of this project.

1.6 SUMMARY

This chapter has laid out the initial grounding for the project and the rest of this report.

The motivation behind this project is the desire to see a convergence of telecommunications, information technology and banking. The Internet evidently provides an infrastructure which can allow a new delivery channel for data, services and goods.

The idea of electronic commerce has been introduced and the project objectives have been set out. It has been explained that the project aims to examine and evaluate all the main issues regarding non-EDI-based commerce.

It has also been shown that the project aims to be readable by a cross-section of users, but is aimed mostly at the research community and users who may be experimenting with the idea of accepting e-cash in lieu of credit or debit cards.

A brief overview for each chapter has been given to aid the reader.

CHAPTER TWO

BACKGROUND INFORMATION

2.1 THE FUNCTION OF MONEY

The Internet provides a new opportunity for commerce and banking. For the potential to be adequately realised, the key issue of a payment system - of money - needs to be investigated and addressed. Without an efficient means of payment many of the opportunities of the medium can immediately be labelled as uneconomic.

To understand what electronic cash is, it is important to understand the functions of a physical currency. Money has four basic functions [HAR]:

- A Unit of Account. The unit of account does not have to have any physical reality. One example of this is the pricing of contracts on LIFFE (London International Financial Futures and Options Exchange) [LIF] in European Currency Units (ECU's).

- An Acceptable Medium of Exchange. Money is useless as a medium of exchange unless it is acceptable to both parties in a transaction.

- A Store of Value. The value of a currency must remain constant. A ten pound note issued in 1975 is exchangeable for a ten pound note issued today. We must note that inflation will always erode true spending power.

- A Means for Deferred Payment. In order for a society to function it must support contracts between parties that include provision for future payment.

When money is implemented on an electronic medium, it is important to keep these functions in mind.

As stated in Chapter 1, we have already seen the development of electronic money. It flows daily around the world as BACS (Banks Automated Clearing Service) payments. BACS currently moves trillions of Pounds and Dollars every day via private networks - but this is institutional electronic money, with little or no use or availability to an Internet user.

In the United Kingdom, the total of sterling accounts held with banks is around ten times the total of notes and coins in circulation. Money supply is therefore essentially bank deposits only fractionally backed by currency, and the currency is backed by nothing at all. As Figure 1 shows, physical money (as indicated by M0) is now less than 4% of the broad money supply (indicated as M4). It can possibly be implied that we are therefore moving towards an electronic commerce based society

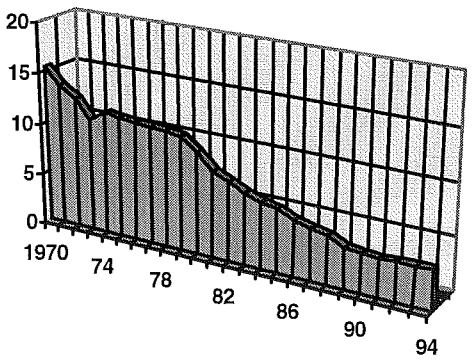


Figure 1: The Percentage of M0 to M4

2.2 SHORTCOMINGS OF PRESENT SYSTEMS

In the past few years, great advances have been made in automating many of the labour-intensive, paper based aspects of commerce. Many corporations are now using electronic data interchange (EDI), e-mail and electronic financial networks that speed up the transfer and settlement of funds. There are many advantages to using these systems, but it is evident that electronic commerce is not a favoured method of making payment. If business does not accept a payment mechanism, then it is unlikely that consumers will ever see it. One reason that the current systems are not widely implemented is because most of them require an actual exchange of paper. Another disadvantage is that the present approaches are not well integrated, open, secure or user-friendly.

Some of the specific shortcomings of systems such as EDI are:

High Cost - The current electronic commerce implications are very costly to develop, maintain and upgrade. There are many variations and inter-operability is not high. The high cost of entry effectively acts as a barrier to allowing micro-payments. Micro-payments are payments that generally cost more than to administer than their actual value. In this project a micro-payment is described as any payment less than £2.00.

Strict Requirements - EDI is unique in that it requires previously established arrangements to allow for a transaction. It also generally requires proprietary software, implying that a manufacturer supplying two companies may have to install two separate EDI lines.

Partial Solutions - Only a small part of the transaction process is automated with EDI. There is no ability to support other functions such as delivery, or even integrate the software with a program that adds functionality.

From this short list it can be seen that on-line commerce needs to take a big step to become generally acceptable.

2.3 HISTORY OF THE INTERNET

The tremendous growth of the Internet, and particularly of the World Wide Web (WWW), has led to a critical mass of businesses and consumers participating in a global on-line marketplace. Quite surprisingly, adoption of the Internet as a commercial medium has been a rapid process with many firms experimenting with on-line catalogues, merchandise information and on-line purchasing. The use of this technology by the majority of major corporations prove that the future of the technology is secure. The Internet is expanding beyond its past use as just a communication medium towards being a completely new market for corporations to target.

The most exciting commercial developments are occurring on the World Wide Web. The WWW is a distributed hypermedia environment within the Internet that was developed by scientists at CERN, the European Particle Physics Laboratory. Its strength lies in the fact that it is easy both for the user and for the information provider to master and is very user-friendly. Its popularity as a commercial medium is mainly due to its ability to facilitate global sharing of resources. It has true potential of providing an efficient channel for global commerce, distribution of information and for sales and marketing.

There is currently a surge of interest in information-based commerce, which is fuelled mainly by the various technologies supporting the web, including Hypertext Mark-up Language (HTML), the Hypertext Transfer protocol (HTTP) and a growing amount of hypertext client and server engines.

Laufman [LAU] suggests that the web has some limitations in its present form. Among these is the ability to provide bandwidth to throughput guarantees. This effectively implies that no provider or customer can expect to grant or receive quality-of-service guarantees. In addition Laufman states that three other existing networks, including telephone, satellite broadcast and cable broadcast may play important roles in the future. The effect these will have on Internet commerce remains to be seen.

The number of people who use the Internet to communicate and share information electronically is expected to grow from 40 million users today to 200 million users in the year 2000 [IDC]. This explosive growth should result in the creation of new Internet-related markets that provide a range of services from simple Internet access to services and software facilitating electronic commerce.

Electronic commerce is already with us and growing steadily. People are shopping over the Internet using credit cards, they are buying shareware from service providers and can even buy sports and theatre tickets with their debit cards. However, there is one major problem. These are all just processes that are no different from transmitting credit card numbers over the telephone, which is not a major problem, but does not solve any of the problems associated with the payment mechanisms that they promote.

The ability to transfer cash over the Internet has the possibility to deliver a blow to current spending methods (such as cheques) and means that the existing spending patterns vis a vis debit, credit and charge cards may be changed for ever. Any single person who has access to a computer, a modem or an Internet link and some simple money management software should be able to carry out a wide range of payment transactions. The implications of this are phenomenal. In one scenario, people would not need or expect to leave their house to buy goods. This could lead to the closure of all High Street shops and banks, with people able to do all of their everyday business securely over the Internet.

From the table below, it can be seen that market analysts predict that in 10 years time as much as 20% of all household expenditures will be funnelled through electronic means:

Purchases	**1994**	**2000 (estimate)**	**2005 (estimate)**
Traditional	$5,150 Billion	$8,500 Billion	$12,000 Billion
E-cash	$245 M	$1,650 B	$2,950B
E-cash via Television and Cable	$45 B	$400 B	$650 B
E-cash via business to business	$140 B	$450 B	$650 B
E-cash via Internet	Negligible	$600 B	$1,250 B
E-cash via other on-line commerce	$60 B	$200 B	$400 B
E-cash share of purchases	4.5%	16%	20%

Source: 1995 US Commerce Department, Killen and Associates

Table 1: Predicted consumer spending of E-cash

2.4 CURRENT RETAILING OVER THE INTERNET

The explosive growth in commercial use of the Internet has been catalysed by the general availability of the World Wide Web and its popularisation by Netscape's, Microsoft's and to a lesser extent NCSA's Web browsers. These software products have made the Internet accessible to everyone and made it easy and relatively cheap to publish material on the Web. The programs are recognised for their ability to give a best effort service across multiple software and hardware platforms, making it easy to publish on the Web.

Many companies have grasped this fact and established home pages on the Internet that although basic, demonstrate that they are willing to experiment with new technology. Some sites have already begun to treat the Web as more than an advertising medium.

This is particularly evident in the United States where the rush to try new ideas is normally more pronounced. However, the United Kingdom has lacked behind. This is not to say that British companies are not willing to experiment. Many High Street companies including Argos [ARG] and Tesco [TES] are now on-line and accepting limited credit card payments for home delivery goods.

2.5 OPPORTUNITIES

In order to assess the opportunities for electronic cash, the role that physical cash plays has been examined. There are other factors that need to be taken into account. The first of which is that despite the technological advances in cards and sophisticated bank systems, coins and banknotes remain the simplest and most acceptable means for most low value transactions.

It has also been noted that cash is predominant at relatively high prices. In the UK, three quarters of payments above £1.00 are made in physical cash - with the rest split between cheques, standing orders, direct debits, credit cards and debit cards. For transactions over £5.00, the proportion made in cash appears to be in free-fall compared to other forms of payment. In Europe, cash transactions account for 80 per cent of the 200 billion payment transactions that are made every year [APA].

The costs associated with these transactions amount to US$35 billion a year. This huge expense is a clear reason to switch away from cash. The biggest problem of this is actually getting people to do this. Research from 1989 has shown that in Europe, some countries were more keen to go 'cashless' than others. In Germany, 95% of people preferred cash, compared with only 45% in France [RBR].

Paper cash also carries one major drawback - that of counterfeiting. Although note printers such as De La Rue PLC are constantly innovating, technology such as colour photocopiers have given potential fraudsters a new weapon, although there are apparently built-in safety features.

People are becoming used to change. This is evident in the growth of new payment methods such as debit cards and electronic funds transfers. At the same time, the use of cheques is falling in most developed countries as they are expensive to process. One important issue is that processing credit or debit cards is also not cheap, with figures showing that payments below around US$2.25 are not viable [RBR].

It can be seen that cash has some clear limitations. The opportunities are potentially there for other transaction methods.

2.6 SUMMARY AND POSSIBLE ADVANTAGES

Electronic commerce has substantial possible advantages over traditional physical payment systems:

- For customers it can reduce the time between outlay of capital and receipt of goods, services or data.
- It can also enable increased responsiveness to customers, as a direct result of the availability of on-demand information delivery.
- It may decrease the time and cost of looking for an item and having it delivered, although this may not be quantifiable.
- It will give the customer the choice of customising services and goods.

For merchants the potential benefits include:

- The potential expansion of the marketplace from local and regional interest to national and international markets with minimum outlay.
- It possibly enables just-in-time production of goods and just-in-time production of payments, thus shortening payment processing times.

The types of products being sold are diverse, ranging from on-line information and services to physical goods. It can possibly be said that what, where and when the merchants deliver have a bearing on the types of payments that will be made, how the payments are captured and how they are settled. Although the market is still in its infancy, Internet merchants represent a diverse set of requirements. Some companies are experimenting with on-line ordering while others are using and on-line payments.

In summary, the combination of cheap computing power, cheap global communications and a reliable and secure money scheme may allow commerce to flourish electronically. As electronic commerce becomes a larger fraction of total commerce then the need for a trusted payment system grows.

CHAPTER THREE

ELECTRONIC PAYMENT MODELS

3.1 THE RISE OF THE INTERNET

Many industry aware companies have been predicting a continuing increase in the number of domestic and commercial Internet users and with it a rise in the electronic marketplace as a significant component of the world economy. Concerns have been expressed over the lack of a suitable payment mechanism as a direct constraint on the expansion of the marketplace.

It is therefore necessary to research and model mechanisms on to which an Internet payment method could be mapped. The following chapter contains the findings. Each of the following payment models implies that there are costs associated with a transaction. It is necessary to note that this implies that different markets exist for different Internet payments. They are:

Micro-payments: These may include pay-per-view articles and information, access to a Web site or a download fee for a piece of software. The charges may be for one Pound or less and are generally too small to warrant the transaction costs of some payment systems.

Macro-payments: These generally are large purchases but can range from under five Pounds to thousands of Pounds. The purchase price is large enough to warrant a cost for each transaction.

3.2 ELECTRONIC PAYMENT MECHANISMS

The current use of physical money can easily be used as a basis to start modelling payment mechanisms. After closely investigating the marketplace, I believe that most mechanisms are able to be classified under one of the following 'real world' paradigms:

CREDIT / DEBIT

> The credit system centres around arranging an account, such as a credit card, and being billed in arrears. A credit limit must be arranged in advance and cannot generally be breached. A debit system works in much the same way but instead is centred around having a pre-paid account. Within a debit system funds can only being used if they are available.

CASH

> Cash can be regarded as a reusable asset that is generally accepted by a large marketplace. Funds can only be used if they are physically available.

TOKEN

> A token is a pre-paid form of exchange. Examples of tokens include phone cards and travellers cheques.

In practice, a credit or debit based system would carry on using existing card details and use the Internet as a secure communications channel. This is not strictly electronic cash, however it will be included in the rest of this research paper as it shares many things in common with the digital cash arena and introduces us to many worthwhile concepts. It must also be noted that it is impossible to transfer physical cash over a computer network, so the 'cash' paradigm above is therefore a modelling of a possible electronic variant.

On the following pages are models of each payment method, detailing the electronic commerce mechanisms that are in use. The mechanisms have been divided into the above headings - Credit and Debit, Cash and Token. A short explanation of each is included, to enhance the understanding of the diagrams.

3.3 TRANSACTION MODELS

3.3.1 Post-paid Model

Transaction model one is the post-paid mechanism which is modelled on credit and debit card transactions.

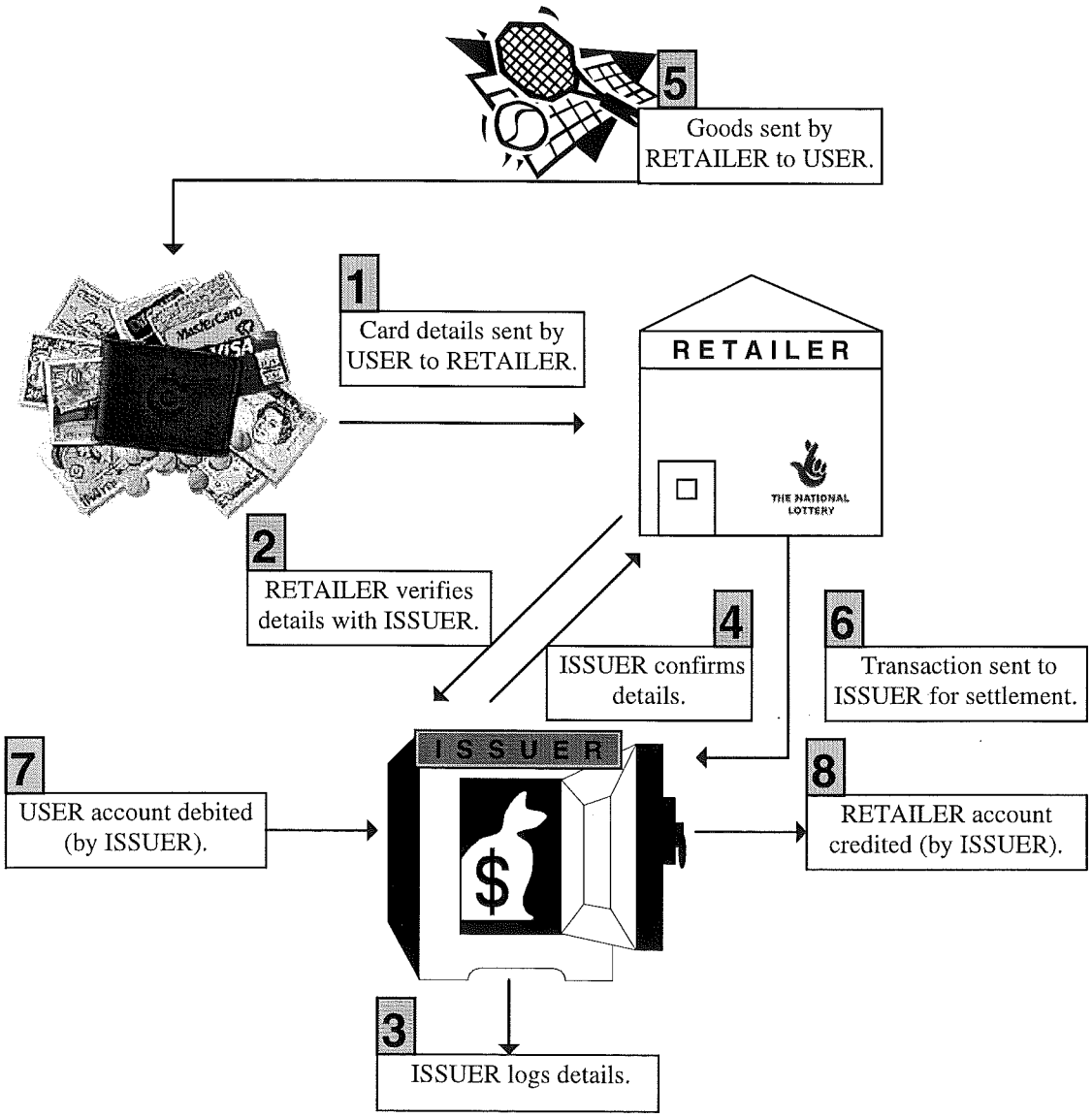


Figure 2: The Post-paid Model.

Figure 2 shows a system which is most widely implemented in credit and debit payment mechanisms. Like its real life paradigm, the system offers the usual benefits of a card transaction such as immediate payments yet also falls to the problem of incurring transaction costs, which although not inherent in the above model, IS implied. This means that there is a minimum transaction threshold below which a transaction is not economically viable for the merchant. The system, like a normal credit card transaction, can only be completed with a merchant that has been authorised by the payment issuer.

3.3.2 The Cash Model

Transaction model two is the 'cash' mechanism which is based on a standard cash transaction.

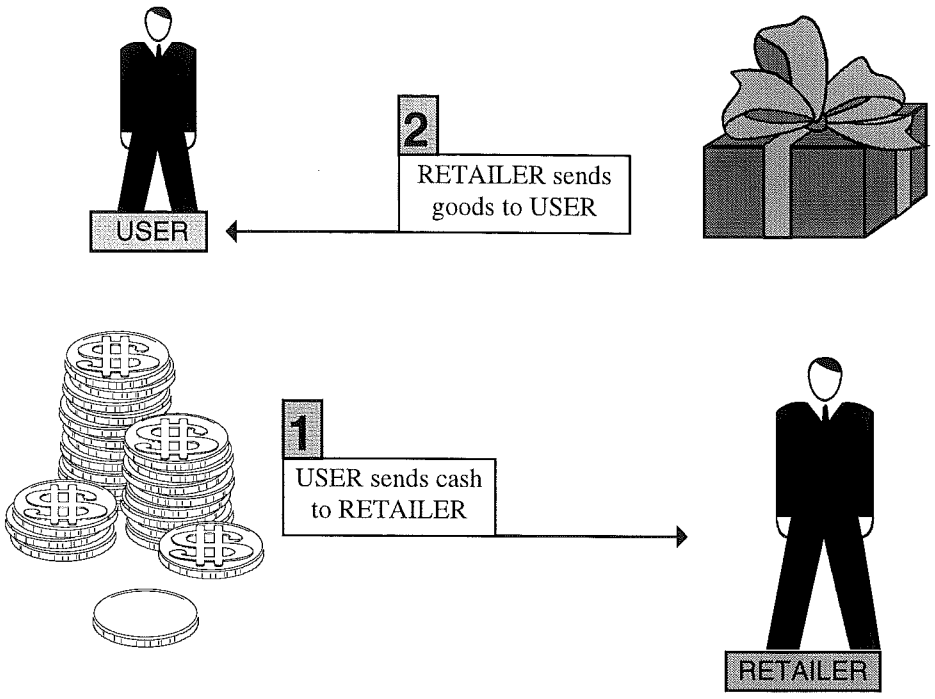


Figure 3: The Cash Model

The cash model allows the transfer of cash between two parties, be they individuals or merchants or a combination of the two. The cash exchanged is completely tangible and can be used again for further transactions. This means that there is no central register and no need to return the payment method to a particular issuer. A feature of this mechanism is that there is no transaction or running costs and therefore there is no transaction amount that is not economically viable.

As there is no central processing, security should be built in to hardware or software and will therefore be completely transparent to users. One drawback is that in effect this means that if someone loses their payment ID then, like cash, it can be used by anyone else.

3.3.3 The Pre-paid Model

Transaction model three is a pre-paid model which is based on token usage as a payment mechanism.

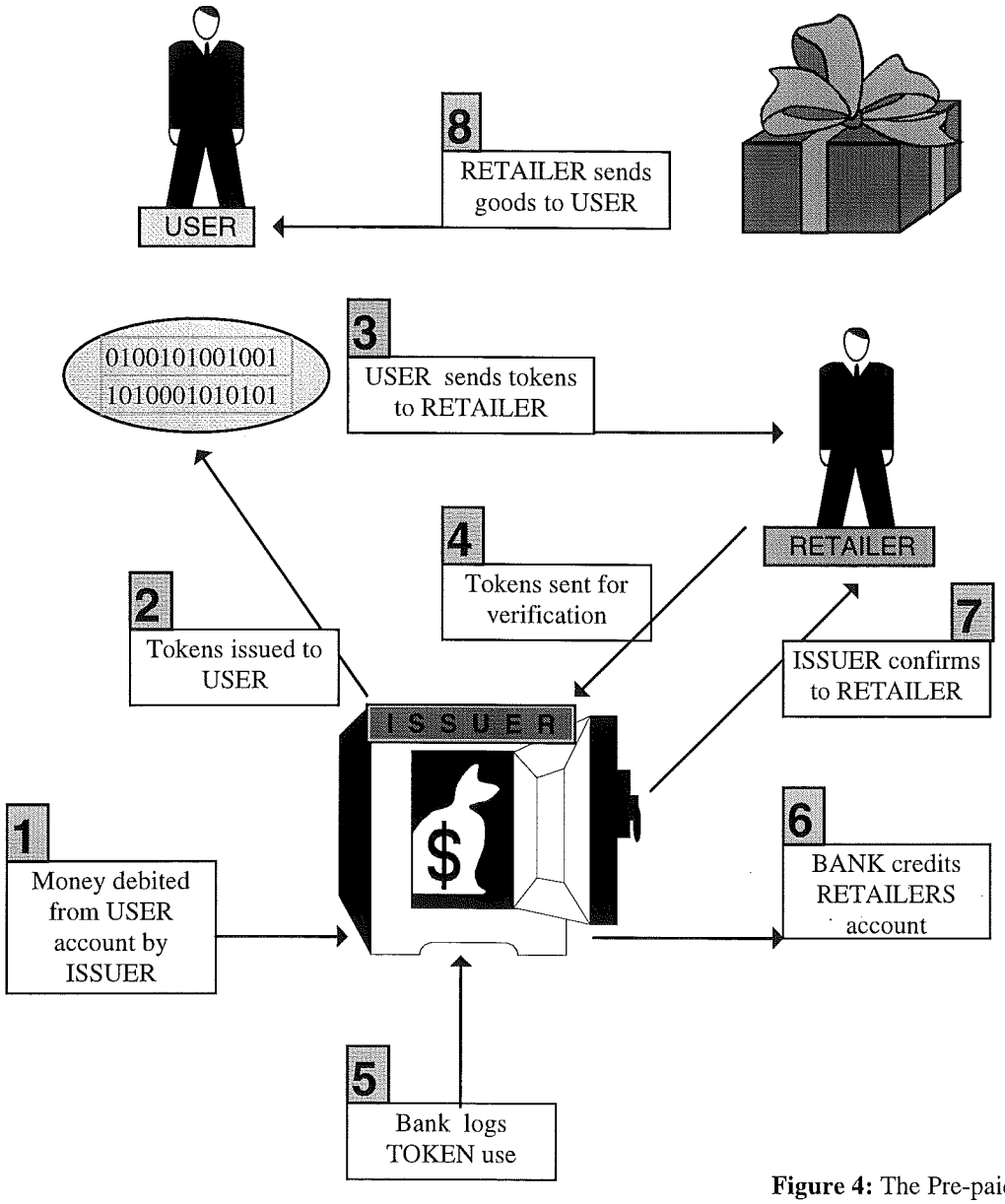


Figure 4: The Pre-paid Mechanism

This mechanism also allows transfers between users, as well as to merchants. The system revolves around pre-paid tokens which can be used for cash at an issuing bank. Like the debit and credit system, there is central transaction processing and therefore associated transaction processing costs. This again means that there must be a minimum transaction value to make the payment economically viable.

Each and every transaction relies on being centrally processed and this is a concern. If a particular network is busy then there is likely to be bottlenecks which in turn could lead to smaller sales figures as consumers abandon the payment method.

The Economist [ECO] alternatively states that with tokens 'what travels from buyer to seller is not merely information that will enable them to settle a transaction subsequently by other means, but something much closer to money itself - a proxy, as it were, for the money with which a card was purchased'.

3.4 SUMMARY

These three mechanisms are based on systems that are available and are in everyday use. It is not necessarily the case that these systems are the best way to tackle the issue of electronic Internet commerce. They are however based on trusted mechanisms i.e. cash and credit cards and are potentially more likely to be championed by regular consumers. It is well documented [LLO] that consumers are adverse to change therefore it may be considered that a system based on a credit card number may prove to be the most successful.

Each system studied has its advantages and disadvantages. In summary, they are:

Transaction Model One: Post-paid.
The Credit/Debit Model.

+ immediate payment to merchant
+ deferred payment for consumer
+ uses highly secure transaction protocols

- transaction costs
- no user to user transactions
- needs a verification network to run concurrently
- transmission protocols are built in

Transaction Model Two: Cash.
The Cash Model.

+ immediate payment at both ends
+ no transfer costs
+ anonymity (if serial numbers are ignored)
+ no audit trail
+ user to user transactions
+ no central processing
+ security mechanisms are independent of transmission protocols used
+ no prior arrangement needed to use

- immediate debit of consumers funds
- no audit trail
- no refunds if 'cash' is lost
- forgo interest costs

Transaction Model Three: Pre-paid.
The Token Model.

+ user to user transactions (via central server)
+ currency can not generally be 'lost'
+ security mechanisms are independent of the transmission protocols being used

- must be pre-purchased
- central transaction process means bottlenecks

It would be unwise to state immediately that one model is better than the other by simply looking at this summary. Adding depth to the argument involves looking at various issues concerning each of the payments. This approach is begun in the next chapter.

CHAPTER FOUR

SECURITY

4.1 DIGITAL SECURITY

Academics are well aware that the TCP/IP protocol is severely lacking in the security department. Drawing on Bellovin's [BEL] work, it is evident that there are some basic areas that can be used to secure illicit information:

Authentication: There is no protocol in the TCP/IP suite that contains any authentication of the communicating parties. Therefore it is virtually impossible to accurately determine whether the addresses in data packets are genuine or not. This makes it easy for one system to impersonate another.

Lower-layer protocols: Many low level protocols are broadcast based (including Ethernet). As such it is possible for any computer on a LAN to eavesdrop on traffic destined for other machines on the same LAN. If we scale the problem up, it can be seen that it is possible for any machine on the Internet that happens to be in the path of two communicating machines to eavesdrop on traffic as it passes.

Similarly in 1983 Voydock and Kent [VOK] described attacks that appear on computer networks and surveyed countermeasures. The threats included eavesdropping, impersonation, denial of service, modification of messages and traffic analysis.

These are just two of the issues. It can be seen that each and every digital cash user who wants to exchange goods for a particular currency will be concerned with the particular security arrangements for the mechanism that is being used. In the same light, if a merchant wants to accept a payment then he must be assured that the payee is genuine and the currency isn't stolen. Unlike a physical currency, a digital currency (which is only a string of bits) can be copied an unlimited amount of times with no loss of quality and signatures can quite easily be copied from one transaction to another. The bits of a signature can be re-arranged without anyone knowing and this is a major cause of concern.

Before we look at security within individual payment mechanisms I shall endeavour to explain cryptography. Cryptography comes from the Greek words ΡΨ]Ξ∴Ω (secret) and ΚΨΙΩΟ (writing) and provides users with the ability to send information between each other in a way that prevents others from reading it. Within digital commerce it is used to represent information as numbers and to mathematically manipulate said numbers. It is also used for authentication to verify users identities and for integrity checking, which is ensuring that a message is not altered since leaving its source.

The mathematically manipulated numbers are known as digital signatures and they can simulate every feature of a manual signature. Digital signatures can only be produced by someone who knows a secret-key, yet they can be seen and checked by anyone. The strength of these algorithms is that they cannot generally be reverse engineered, i.e. the mathematics behind the signatures are strong enough to prevent anyone from forging the signature without the secret key.

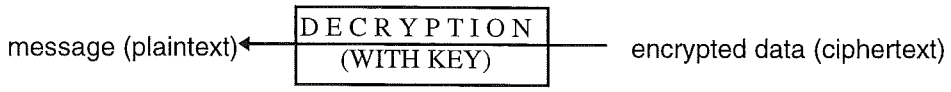
Many digital signatures are created from using the results of various algorithms, the most used of which are described in detail on the following pages.

There are 3 types of cryptographic functions: public-key functions, secret-key functions and hash functions. Whereas public-key encryption encompasses the use of two keys, secret key functions only use one and hash functions don't use any. In essence this mean that there is a security algorithm which has no secret-key. This will be explained later.

4.2 PRIVATE KEY ENCRYPTION

A private key encryption system is a system that allows data to be scrambled so it can only be understood by someone who knows the private key. Given a message and the private key, the data will be encrypted into seemingly random data which is exactly the same length as the original message.

Similarly, decryption uses the same key:



In its simplest form a user could say that the key was $n + 1$, where n is a letter of the alphabet. Thus the encrypted version of the alphabet would look like this:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Unencrypted:	a	b	c	d	e	f	g	h	i	j	k	**l**	m	n	**o**	p	q	r	**s**	**t**	u	v	w	x	y	z
Encrypted:	z	a	b	c	d	e	f	g	*h*	i	j	k	l	m	*n*	o	p	q	*r*	*s*	t	u	v	w	x	y

Figure 5: An Example of Private Key Encryption

It can be seen that the unencrypted word *lost* becomes *knrs* when encrypted. However, in digital cash systems the key is a much larger number that is needed to both lock and unlock the data. There are major security uses for this technology. They are:

4.2.1 Integrity of Data Transmission

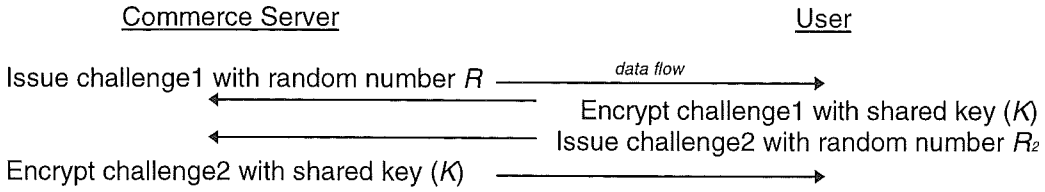
If two users agree on a private key then by using secret key cryptography they can securely send messages to each other. A commerce server could send data to a user over an insecure network without worrying about people intercepting the data, as any data that gets intercepted will be in an unintelligible format. This can be seen in the diagram above.

4.2.2 Secure Storage (on Insecure Media)

Information that needs to be preserved on local media but is essentially insecure can be encrypted using a private key. When the data is retrieved it has to be unencrypted. This means that however easy the data is to get hold of it will be unintelligible. However, once the private key is forgotten the data is irrevocably lost.

4.2.3 Authentication

Private-key technology enables the use of strong authentication. Strong authentication ensures that two users can prove knowledge of a secret between each other, without actually revealing it to each other. This has uses when for instance, a secure commerce server has to interact with a user over an insecure network. An example of the data interchange is shown on the following page.



If we assume a scenario where the Server and the User share a key K and they wish to authenticate that they are communicating with each other. They each would pick a random number (R, R_2) to challenge each other with. If the data exchange is completed successfully, then both the server and the user have proven that they know they know K without revealing what K was. One major disadvantage of this approach is that the random figure must be suitably large so that a particular challenge does not have much chance of appearing twice. If the random number is taken from a smaller space then there is the opportunity for a third party to challenge the server by impersonating the User and thus receiving encrypted data in return. This could then form the basis for an attack on the system.

4.2.4 Integrity Check

A private key crypto-system can be used to generate a fixed-length checksum associated with a message. Given a private key and some data a cryptographic checksum algorithm produces a fixed-length message integrity code that can be sent with the data. These codes have been used to protect the integrity of large interbank fund transfers for some time [KPS].

4.2.5 Data Encryption Standard

An example of a more complicated private key system is knows as the Data Encryption Standard (DES). It is based on an IBM system called Lucifer, and in its current form is fully approved for non-classified use by the US government.

In DES data is encrypted in 64 bit blocks with a 56 bit long key. The algorithm scrambles the data 16 times by splitting the 64 bit block into two 32 bit halves (l_n, r_n). The key (k) is then used to scramble one half of the block which is passed through an equation called the s-box, which is a random function. The second 32 bit half is then used to encrypt the first half. This is repeated 16 times to ensure strength of encryption [DES].

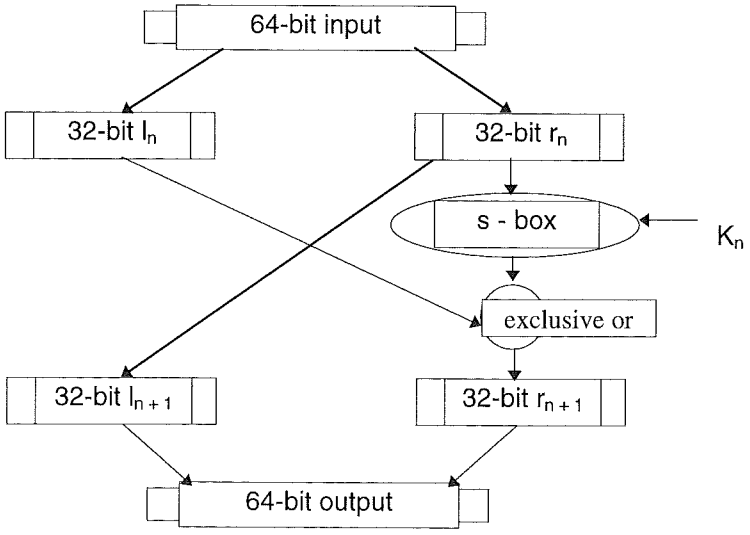


Figure 6: One Round of DES Encryption

4.3 PUBLIC KEY ENCRYPTION

Public key algorithms have two separate and independent keys which are used independently to lock and unlock the code. The key that locks the data cannot be used to unlock it, and vice versa. The benefit of this system is that two people can communicate safely without needing to meet to discuss a secret key.

The idea is simple. Each user publishes one of their two keys (the public key) and keeps the other key secret. Each then uses the others public key to encrypt the message. Thus, only the holder of the real private key can decode the message.

Similarly, decryption is the inverse function of encryption, this time the private-key is used.

Public key algorithms are already in use as digital signatures. When someone sends an e-mail message, they can encrypt their signature with their private key. Anyone who knows the public key can decrypt the message to ensure it is genuine.

The public key is thus needed for decryption:

There are major security uses for this public key cryptographic techniques. Here is a summary of its major uses:

4.3.1 Integrity of Data Transmission

This encryption method allows for a currency issuer <public key = CI_{PUB}, private key = CI_{PRI}> who knows a users public key to transmit data safely to that user <public key = US_{PUB}, private key = US_{PRI}>. In this case it can be seen that:

Currency Issuer (CI)		User (US)
encrypt *message1* using US_{PUB}	>>>>>>>>>>>>	decrypt *message1* using CI_{PRI}
decrypt *message2* using US_{PRI}	>>>>>>>>>>>>	encrypt *message2* using CI_{PUB}

4.3.2 Secure Storage (on Insecure Media)

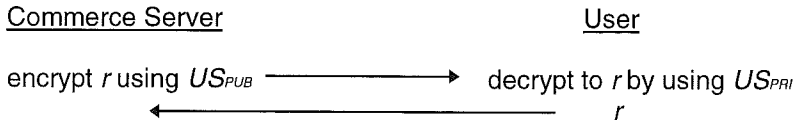
In the same way that with private key cryptography the user encrypts data with a private key, public key encryption means encrypting the data with the public key. In this instant however, decryption takes place with the private key. This method does have an advantage over private key technology as the user does not have to provide the key to the computer that encrypts the data. Once again, if the key is lost or forgotten the data is irrevocably lost.

4.3.3 Authentication

Public key technology authenticates users in an easier manner than private key cryptography. If we assume that the Commerce Server knows the Users public key and it wants to identify the users identity, then:

Commerce Server picks a random number (r).
The number is encrypted using the Users public key (US_{PUB}).
The result of the encryption is sent to the User.

The User decrypts with the private key US_{PRI} to authenticate and sends the random number r back to the commerce server. This is modelled below:



4.3.4 Digital Signatures

Digital signatures provide two major services. They prove who generated the data, and they prove that the data has not been modified in any way by anyone since the message and digital signature were generated.

The benefit over private key based cryptographic checksums is that they include non-repudiation. It can be proved that some-one sent a particular command or particular data over a network, because the signature is always generated with a private-key.

4.3.5 The RSA Algorithm

One example of a public key encryption algorithm, and probably the most widely used is known as RSA. It was developed by three MIT fellows (Rivest, Shamir and Adleman) and is now owned by RSA Data Security Inc. [RSA]. RSA encrypts and decrypts by raising numbers to a power modulo a number which is the product of two large prime numbers. The two primes are kept secret. The key length in RSA is variable. This means that a user can choose a long key length for security conscious systems or a short key for efficiency in encryption and decryption. RSA security lies in the problem of quickly factoring a large number. Factoring is a slow and arduous process.

The system works by utilising the following steps.

Firstly, a public and corresponding private key are needed, both of which need to be large primes p and q and both of which are kept secret and are over 128 bits long. These numbers need to be multiplied together to get n. A personal public key is generated from a number e that is relatively prime to $\phi(n)$. Since p and q are known, then $\phi(n)$ is known to be $(p - 1)(q - 1)$. The personal public key is therefore $<e,n>$. The personal private key is the number d that is the inverse of e mod $\phi(n)$. The private key is therefore $<d,n>$.

To encrypt a message m, someone using the personal key should compute ciphertext $c = m^e \bmod n$. Only the user will be able to decrypt c, using the personal public key to compute $m = c^d \bmod n$. The message m must be smaller than the result of multiplying the two primes n.

4.4 HASH ALGORITHMS

Hash functions can be used to ensure that a file arrives in the same condition as which it was sent. Hash algorithms take a large file and reduce it to a short number (of fixed-length) so that the short number can be used in place of the long file. It is therefore a one-way function. There are two main properties of a secure hash algorithm:

- All possible short numbers are equally probable to be the outcome of a hash function.
- It is infeasible to recreate a file that generates any given number.

The basic idea of a message hash is that the input gets mangled so well that the process is impossible to reverse engineer. An example of a hash may be:

> Take some data *d*, treat it as a number, add the square root of a random number *r*, square the result, and take the beginning and end *n* digits as the hash.

Whereas this is computationally not difficult, there is no obvious way to produce a replica of the hash number. However, the hash function does has to have a certain number of bits to ensure effectiveness against someone being able to find two datagrams with the same hash number. If the message hash has *m* bits, then it would take a reasonable $2^{m/2}$ datagrams, before the same value could be found. Thus the only effective hash would have an output of 128 bits or more, as general computing power is not currently able to efficiently and effectively search 2^{64} datagrams.

The are numerous uses for hash algorithms. The most ideal are:

4.4.1 Integrity of Data Transmission.

Like private key cryptography, hash functions can be used to generate a checksum to protect data being transmitted over an insecure network. Again, if a password is agreed between a server and a user, the server can use a hash to calculate a checksum for the user by taking the data, concatenating it with the password and computing the hash of the result. The server can then send this hash, as well as the data, to the user. The user can then take the data, concatenate it with the agreed password and then see if the hash is the same. If they are the same then the data was sent by the server.

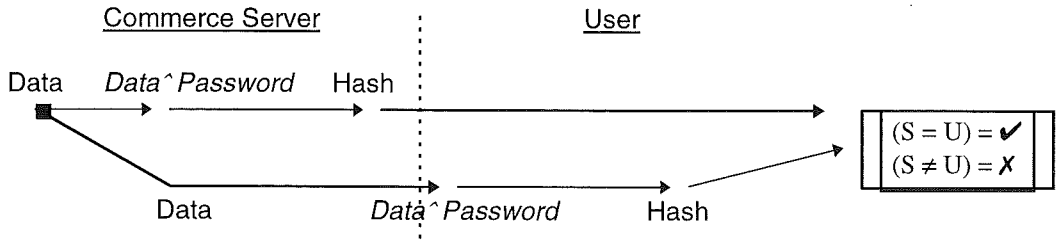


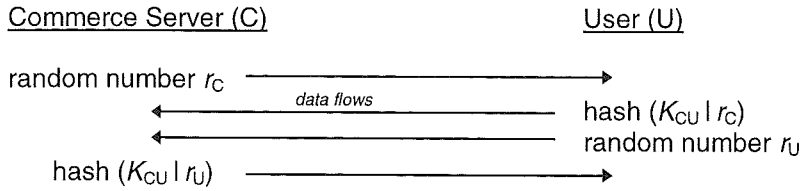
Figure 7: Data Flows for Data Integrity

4.4.2 Digital Signature Efficiency

Public key algorithms generally are very processor intensive. Therefore, to save processor time, a hash of the data can be computed and signed rather than signing the full data message itself. The hash algorithms that do this are much less processor-intensive than private key, and the hash data is much shorter than the message data.

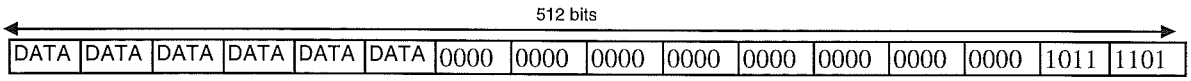
4.4.3 Authentication

Although it is possible to use private key cryptography as an authentication tool, it is sometimes easier and quicker to use a hash function to authenticate one user with another. In place of the 'decryption' of the private key, a data check takes place to ensure that the message hash results match.



4.4.4 MD5 and The Secure Hash Algorithm

MD5 is a hash function devised by Ron Rivest [RIW]. A 128-bit hash value is produced by processing data in 512-bit blocks. As can be seen by the representative diagram below, *n* x 512-bit blocks is broken up into sixteen 32-bit blocks, M_0 - M_{15}. As the last block of data is rarely 512 bits long, data is bit-stuffed in the following way:



Bit-stuffing is achieved by adding a single bit 1, a flexible amount of 0 bits and a 64 bit number representing the number of bits in the file. After padding the data, MD5 takes four 32-bit variables (*A, B, C, D*) and permutes them in four rounds with the sixteen blocks. When completed, the four values are appended to create the 128-bit hash number.

Taking into account the procedures and functions on the right, the hashing process can be defined as:

1. The file is broken into 512-bit blocks and padded.
2. The four variables (*A, B, C, D*) are set.
3. Each 512-bit block is processed with the four rounds:

(I) A, B, C, D are copied to A_1, B_2, C_3, D_4.
(ii) Function *FF* operated 16 times on A_1 B_2 C_3 D_4.
(Each time a different constant *t*, shift value *s* and block *Mj* is used)
(iii) Function *GG* is used 16 times in same manner.
(iv) Function *HH* is used 16 times in same manner.
(v) Function *II* is used 16 times in same manner.
(vi) A_1, B_2, C_3, D_4 are added back into *A, B, C, D.*

4. *A, B, C, D* are concatenated together to produce the hash number.

The scrambling procedure for MD5 can be summarised in equations as:

FF(a, b, c, d, j, s, t) = a := a + (F(b, c, d) + Mj + t) << s

GG(a, b, c, d, j, s, t) = a := a + (G(b, c, d) + Mj + t) << s

HH(a, b, c, d, j, s, t) = a := a + (H(b, c, d) + Mj + t) << s

II(a, b, c, d, j, s, t) = a := a + (I(b, c, d) + Mj + t) << s

where << stands for 'left shift'.

The basic scrambling functions, F, G, H and I are:

F(X, Y, Z) = (X ⊗ Y) ⊕ ((notX)andZ)

G(X, Y, Z) = (X ⊗ Z) ⊕ (Y ⊕(notZ))

H(X, Y, Z) = X ❸ Y ❸ Z

I(X, Y, Z) = Y ❸ (X ⊕ (notZ))

⊗ is a bitwise AND
⊕ is a bitwise OR
❸ is a bitwise XOR

Source: [CRY1]

MD4 [RIV], the precursor to MD5, forms the basis for the Secure Hash Algorithm (SHA). The structure of MD4 was used by the National Institute of Standards and Technology when it created the algorithm for use in its Digital Signature Standard [NIS]. The basis is the same, except that there are five variables in place of four, and that the scrambling functions are slightly different. Other major changes include that for each of the four rounds each function is applied twenty times, as opposed to the original sixteen meaning that some of the 32-bit values are used more than once and a change to the four functions, making them more comprehensive.

4.5 BLIND DIGITAL SIGNATURES

Developed by David Chaum [CHA, USP], blind digital signatures are a way to carry out transactions that are 'unconditionally untraceable'.

For a digital payment system that requires some type of authorisation by a central authority, this system ensures that even if a merchant and the currency issuer collude, that they cannot determine who spent the currency. The following diagram is an example of a typical transaction:

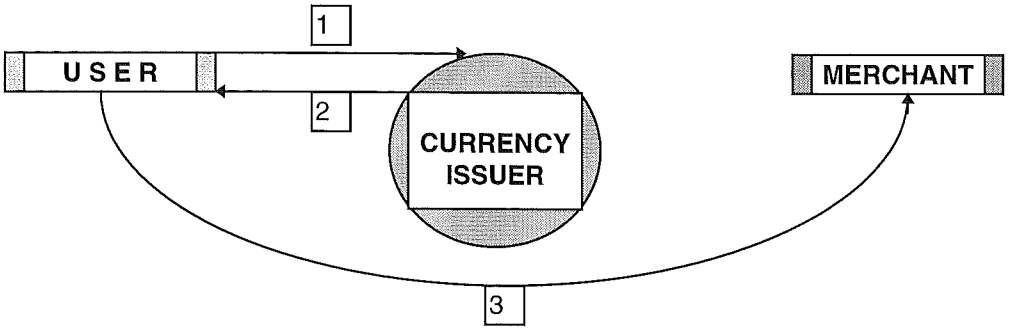


Figure 8: Blind Digital Signatures

By sending the digital currency number to the issuer for signing (1), the user in essence multiplies it by a random number. Consequently the issuer knows nothing about what it is signing (2) except that it carries the user's digital signature. After receiving the blinded note signed by the issuer, the user can divide out the blinding factor and use the currency as per normal (3). Because the bank has no idea of the factor that is used for blinding, it has no way to link the currency number that the user is spending to the currency number that the merchant banks.

Chaum, Fiat and Naor [CFN] proposed a method for generating blinded notes that requires the User to answer a random numeric query about each digital currency number when making a payment. Spending such a currency would not compromise the anonymity of the system, but double spending it would reveal enough information to make the fraud traceable.

4.6 OTHER SECURITY APPROACHES

The approaches outlined previously are by far the most widely used in the field of electronic commerce, however there are other encryption and authorisation methods available on the market. Here follows an explanation of the remaining common security approaches.

Zero-Knowledge Proofs

Payment systems should have the ability to authenticate themselves without revealing who they are. ZKP is a 'challenge and respond' protocol in which a question is asked and the correct response is required. Therefore it is an ideal solution for proving that a user knows something without revealing any information about the user. The phrase zero knowledge stems from the fact that if the whole conversation is overhead, then no knowledge can be gained. The fundamental discovery of this method was by Goldwasser, Micali and Rackoff in 1982 [GMR].

One electronic cash use of this is that zero knowledge proofs can be used for the authentication of a credit card without revealing the payee or the serial number of the card.

Secret Sharing

The information about a user can be split between *n* entities, ensuring that the information can only be collated when all *n* parts are re-united. The system for splitting the information into smaller entities will not give the holder of one part any details about the information held.

An electronic cash use of secret sharing is as an aid to the prevention of double spending by splitting a UserID into two parts.

4.7 OTHER SECURITY SYSTEMS

RSA, DES and MD-5 are undoubtedly the favourite encryption systems used in electronic commerce. There are other systems that are used, albeit less frequently. Here follows an explanation of the second tier of security products.

Kerberos

Kerberos is a key management system that has a secure server that is responsible for keeping a list of everyone's passwords and secret keys. It is used to establish communications between two machines that have never contacted each other before. In essence, if the server is secure then the connection between the two machines is also secure.

Secure HTTP

Secure Hypertext Transfer Protocol (S-HTTP) is based on HTTP but is security enhanced. It provides four key features: transaction confidentiality, authentication, non-repudiation of origin and message integrity. This is accomplished by adding public-key cryptography from RSA to messaging in the application layer of the ISO model. It also supports secret sharing (above) and Kerberos (above).

Its use in electronic commerce can be as additional level of confidentiality when purchasing goods or home banking over the Internet. A short introduction to secure protocols is given in Appendix B.

Pretty Good Privacy

Pretty Good Privacy (PGP) is a hybrid cryptosystem that combines private key and public key cryptography. It combines the speed of private key cryptography with the advantages of public key that are discussed earlier in this chapter. Its job is to safeguard messages and this is done by a user publishing their public key and then having people transmit messages to them encrypted with that (same) key. In this way it can be seen that only the person who has the private key can decrypt the message. The following diagram explains how PGP encodes and decodes:

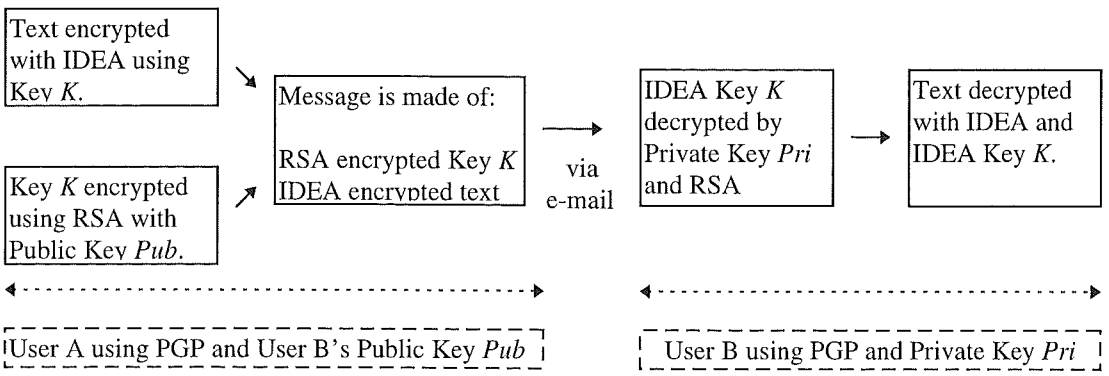


Figure 9: An Overview of PGP

The security of PGP is primarily based on RSA which is mentioned earlier in this chapter. The security of RSA is based on modular exponentiation. We are already aware that RSA can be broken when given enough resources to factor the sum of the two large primes.

IDEA

IDEA (International Data Encryption Algorithm) is a symmetrical block cipher algorithm with a 64-bit block length and a 128-bit key. As it is generally implemented in hardware it has a ciphering capacity which exceeds most DES-based cryptosystems. The security is based on providing a high level of security that is based on the users' ignorance of the secret key rather than keeping the algorithm secret. A specification of the algorithm can be found on the developers Web site [ASC].

4.8 SUMMARY

As the use of computer networks for commerce grows, it is evident that business will frequently be conducted between two parties that have never met each other. Not only reducing customer confidence (by reducing the 'legitimacy' of the merchant), it also makes it harder for the merchant to identify the customers' identity.

Security measures in the form of digital signatures help to ensure the legitimacy of transactions in these cases.

Another problem is that information sent over computer networks can easily be stolen or changed. The best way to protect the confidentiality of data accessed through networks is to use encryption, which is a transformation of data that varies based on an encryption key. Encryption not only protects confidentiality, but ensures data integrity.

There are varied ways to encrypt data based on mathematical formulae. DES and other private key cryptosystems depend wholly on the sharing of at least one secret key between the communicating parties. The keys are generally generated in a secure facility and key parts are distributed to remote network nodes, where a secure repository for keys for all communicating parties on a network must be set up, kept completely up to date and safe-guarded, especially if the data is particularly sensitive, as in the case of electronic finance. This implies that key management with private key systems is particularly time and labour intensive, complex and expensive. It is necessary to question whether the benefits of a system, including extreme robustness and speed of operation, outweigh the associated disadvantages.

Public key cryptography, based on a pair of related keys where one key is public and one is private is a slower mechanism. The key pair can be generated within the public key facility of a network node. Following this, the public key is widely distributed to encrypt messages with, whilst the private key is held securely within the network node.

This implies that with a combination of public and private key systems, that one system can be used to aid the other. On example of this may be to distribute DES keys encrypted with the public key of the intended recipient. In this case, the recipient SHOULD be the only person who has the private key to decrypt the DES key.

When a user encrypts an object with a private key and transmits it, any person can decrypt it (assuming that the public key details are widely available). This ably demonstrates the property of non-repudiation which is the basis for digital signatures, where the user has the only key that could have possibly encrypted some data if the data made sense when decrypted by the senders public key, implying that the sender is definitely the source of the data. A decent system should therefore aim to use DES for encryption and a public key system for digital signatures and key management.

CHAPTER FIVE

PAYMENT SYSTEMS

This chapter contains details of payment systems that are currently available on the Internet. For ease of understanding they have been divided into the three mechanisms that were established in Chapter Three. Each of these systems is either in use or trial. Internet payment systems that were purely hypothetical have been left out.

5.1 CREDIT AND DEBIT SYSTEMS

5.1.1 First Virtual Holdings (http://www.fv.com)

First Virtual Holdings is an on-line bank that has been designed for purchases of on-line services. Users of the system register as a buyer or seller with First Virtual and send them credit card details by post. This gives the user a First Virtual account ID (VirtualPIN), which can be used at any Web site displaying the First Virtual logo. The pre-eminent advantage of this system is that it has been designed with small purchases in mind. Small value purchases are aggregated until a reasonable amount ($10 at time of writing) is reached and then the money is taken from the buyers credit card, with FV taking a small fee.

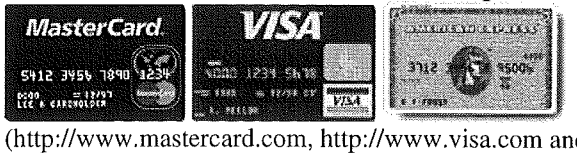
Buyers use their VirtualPIN when buying whilst sellers verify the buyers' details on line with FV and supply the information or data purchased. It is then up to the buyer to verify with First Virtual via e-mail that the transaction actually took place.

Even though International developments are taking place, transactions can only be billed to MasterCard or Visa accounts in US currency. Sellers must also receive funds in US currency, which effectively means that the bank must be physically based in the United States.

First Virtual is just a communications channel for exchanging card details. However, the ability to try a product before it is bought gives it a major advantage above its rivals. This advantage is potentially outweighed by the unknown factor of e-mail delivery and usage. The question must be asked, 'Will the users pay *after* buying the product?' After buying many products on the web, a user may open the e-mail the next day to find multiple messages asking for confirmation of certain purchases. It is too easy to say 'No'. First Virtual states that it will actively investigate and shut down the accounts of those that abuse the system. No metrics are given that suggest the number of 'tryouts' that are allowed.

The system relies on network security to be secure. Its structure is built solely upon network applications including SMTP/RFC822/MIME [MAI], telnet, finger, ftp and http. First Virtual acknowledges that it is easy to fake network addresses and e-mail, but believes that intellectual copyright infringement is much easier to do. This is certainly true.

5.1.2 MasterCard, Visa and American Express



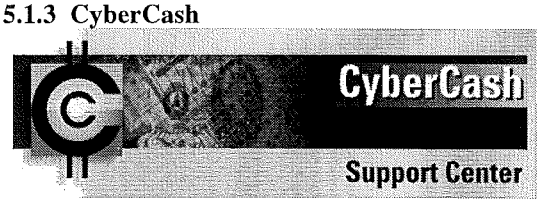
(http://www.mastercard.com, http://www.visa.com and http://www.americanexpress.com)

MasterCard International and Visa International joined together to announce a technical standard for safeguarding payment card purchases made over open networks. Prior to this effort, Visa and MasterCard were pursuing separate specifications. The new specification, called Secure Electronic Transactions (SET), represents the convergence of those individual efforts.

Secure Electronic Transaction has been developed by Visa and MasterCard, with participation from several technology companies including Microsoft, IBM, and Netscape. SET will be based on specially developed encryption technology from RSA Data Security. The specification is open and free to anyone who wishes to use it to develop SET-compliant software, thus encouraging a de-facto Internet standard.

Secure Electronic Transaction (SET) is an open specification for protecting payment card purchases on any type of network. The SET specification incorporates the use of public key cryptography to protect the privacy of personal and financial information over any open network. The specification calls for software to reside in the cardholder's personal computer and in the merchant's network computer. In addition, there is technology residing at the acquirer's (the merchant's bank) location to decrypt the financial information, as well as at the certificate authorities location to issue digital certificates. It is anticipated that software vendors will incorporate SET into existing browsers and merchant servers when Visa's testing is completed.

5.1.3 CyberCash



(http://www.cybercash.com)

CyberCash provides free software to users and merchants implementing their Secure Internet Payment Service that uses proprietary encryption techniques. Accounts are set up by downloading the software from CyberCash's Web site and filling out a simple form which includes details of the credit cards that are to be used. In return the customer gets a public key. Filling out credit card details early in the process means that a user cannot choose to pay with a card that has not been registered earlier, thus ensuring that the card is cleared for use before a transaction is started.

Buyers are able to submit credit card payment to retailers who then pass it on to a CyberCash server linked to a number of US banks' private networks. Within CyberCash, retailers do not get to see the credit details in the encrypted payment.

5.1.4 BankNet

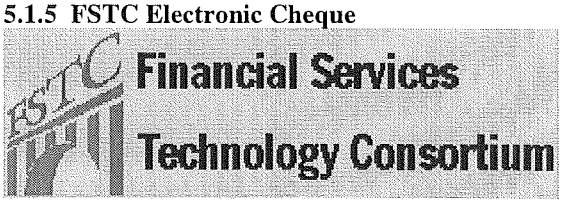
BANKNET

(http://mkn.co.uk/banknet)

BankNet is an on-line joint venture bank created by Marketnet and Secure Trust Bank PLC. The Internet account offers the same features as a normal current account, but with the ability to make transaction queries and submissions on-line. BankNet also provide an electronic payment method known as ECheques, which can be used on the Internet to buy goods and services. This service is Sterling denominated. The WWW browser allows the BankNet account holder to digitally sign the cheques with a private key which must firstly be registered with BankNet. This system is live at the moment, with users able to write cheques to other BankNet account holders. BankNet will soon extend this system to allow users who bank with the 4 main UK clearing banks to deposit BankNet electronic cheques via e-mail.

The bank asks users to obtain a copy of a program that will generate a private key. They generally recommend Workhorse, but Pretty Good Privacy (PGP) is fine. When the user has generated a public key (minimum 512 bits, up to 1,024 bits), the user must set limits to what the key can do. For example this can be a limited lifespan, a limited transaction size or a limited turnover. BankNet state that the Bank of England have requested that transactions are initially limited to £25 or less. After registering the key, it can be used to make and authorise transactions over the system. Users can then check their accounts live on-line.

5.1.5 FSTC Electronic Cheque



(http://www.fstc.org)

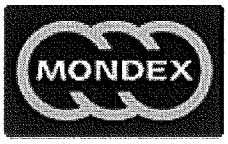
The Financial Services Technology Consortium (FSTC) is a consortium of banks, financial services providers, national laboratories, universities, and government agencies who sponsor and participate in non-competitive collaborative research and development on interbank technical projects.

The electronic cheque is sent by the customer to a merchant, who must be on-line, where it is banked, and the two banks settle with each other by using standard banking electronic clearing and settling systems. One benefit of the electronic cheque is that other flows can be accommodated, such as the customer sending the electronic cheque to the merchant's bank with payment instructions, including the payee's bank.

The electronic cheque consists of an ASCII text block, cryptographically signed by an electronic chequebook, as an electronic mail counterpart to the existing system of paper cheques and physical mail. The consumer has an electronic chequebook which he or she may insert into a PC in order to "write" an electronic cheque for transmission to a merchant. This form of payment will be of particular value in paying for electronic or network services where no previous relationship exists between buyer and seller. The FSTC appears to favour the use of external hardware devices to act as electronic cheque books.

5.2 CASH BASED MECHANISMS

5.2.1 Mondex



(http://www.mondex.com)

Developed initially by NatWest bank with subsequent backing by Midland Bank, Mondex is the first true electronic cash system. It is based on tamper-proof smart card technology that holds cash in multiple currencies. The BT payphones can also be used as Automated Teller Machines, to load cash on to a card from a remote bank account.

The software for this payment mechanism is resident on the smart card and authentication is used. Mondex's security relies on a unique 'digital signature' that is generated by the chip on the card and which can be recognised by the other Mondex card involved in the transaction. This 'digital signature' is the guarantee that the cards involved are genuine Mondex cards and that they are dealing with untampered Mondex signals. This recognition process also identifies the counterparty card for which the cash is intended - so funds cannot be intercepted by a third party without detection. No central processing or central authentication is required, which means that Mondex is not only very simple and efficient to use, but also truly anonymous as no central records of transfers can be kept.

An introduction to smart cards is given in Appendix A.

5.2.2 Conditional Access For Europe (CAFE)

CAFE, like Mondex is creating transfer methods for cash by utilising smart card technology. Whilst Mondex is backed by multi-national banks, CAFE is a mixture of Universities and IT companies including Siemens of Germany, Gemplus of France and DigiCash of the Netherlands (q.v.), thus creating a pool of instant technological knowledge. It is project number 7023 of the EU's 'ESPRIT' program.

CAFE is an experimental system based on smart cards and smart wallets. The smart cards are normal credit card sized and can be used in shops, at ATM machines and over the telephone. The wallets communicate via infra-red. The CAFE protocols are off-line, making the wallets an extremely portable system. In most cases there is no need for terminals to be connected on-line to a central database for transactions although it is also suitable for an on-line central database-terminal system.

This system is very much like Mondex. Money is kept on either a card or on a wallet, with unrestricted transfers between both. In theory, a user should keep a wallet at home, with the majority of the cash on it, and only charge up the card with the minimum amount of money needed. Transactions are unconditionally anonymous so that tracking of individuals' movements and payment methods cannot take place. The cards do however include a way to trace transactions that have taken place in the past. Security is accomplished by public key cryptography, so that if a CAFE card is stolen and the memory is interrogated, then messages will not be able to be decrypted.

5.3 TOKEN BASED PAYMENT MECHANISMS

5.3.1 DigiCash

(http://www.digicash.com)

DigiCash is a Dutch company, headquartered on the National Research Campus for Exact Sciences. The DigiCash mechanism involves the creation of electronic 'coins' that are digitally signed numbers that ultimately are exchanged for physical money from a users bank account. These coins can only ever be spent once. DigiCash use an electronic 'cheque', which is a single number that contains multiple denomination terms sufficient for a transaction up to a pre-determined limit, and to which the appropriate value is assigned at payment time. The valuation of the denomination can be made variable (i.e. 20p can be made up of 2 x 10p's or 1 x 20p). This system means that a bank does not need to issue a multitude of different currencies. One major advantage of this system is that the values of the denomination terms can be made variable. Cheques can therefore be spent in different currencies.

DigiCash have also patented many forms of hardware. Rather than having accounts debited at a bank, customers can transfer national currencies into terminal equipment such as smart cards and PC's. When a DigiCash coin is spent it is immediately sent by the recipient to the issuing bank for on-line verification and logging before confirming receipt to the payer, who then discards the used coins. The appropriate amount is then credited to the payees account.
Much of the effort behind the system has been spent ensuring that coins can be verified without revealing the identity of the buyer to the bank or the payee. However, all transactions are centrally logged and all received payments are paid into the recipients bank so that the only anonymity gained is by the payer of any individual transaction.

5.3.2 NetCash

NetCash is an electronic token-based payment system that is especially suitable for the purchase of low cost items such as data and information. It is based on 'payment coupons' that may be traded via e-mail, inferring that information providers and merchants may operate their businesses completely via this medium.

Users can access the 'NetBank' and make purchases from anywhere on the Internet. Users also have the choice of sending unencrypted mail, which is very insecure, or PGP encrypted mail. Since the ownership of NetCash is based on the knowledge of a unique serial number embedded into it, it is unmistakably a good idea to use encrypted mail wherever possible.

NetCash is purchased from the NetBank by sending US Dollar denominated funds to the NetCash office in exchange for the payment coupons. One major advantage of this approach is that you can e-mail NetCash details of your cheque account and they will automatically 'cash' that cheque into NetCash currency immediately. The coupons that are issued are assigned a 'pending payment' status until the cheque is cleared, although the coupons can still be spent. One disadvantage of this system is that NetCash coupons appear to be only accepted one at a time or the system becomes confused.

5.4 SUMMARY

Each of the many payment mechanisms that are currently available can be classified in one of the three headings modelled in Chapter Three:

- Credit / Debit
- Token
- Cash

There are a magnitude of Internet payment mechanisms vying for a slice of the Internet payments' marketplace. Secure credit card transaction schemes such as CyberCash and the MasterCard, American Express and Visa combination are one way forward for electronic commerce. When using these systems, the users credit card number is encrypted using asymmetric cryptography so that it could only be read by a merchant. There are of course legal issues such as whether an encrypted card number is as binding as a signature, but these are considered to be outside the scope of this project. Because of the costs associated with clearing credit card payments through the existing private financial network, this mode of payments is not well suited for micropayments as the cost of transactions is more than the payment amount (unless they become subsidised).

Payment systems such as First Virtual and NetCheque let customers maintain accounts on a payment server and authorise charges against those accounts. An important advantage of systems like this is the low transaction cost. This is critical if such systems are to support micropayments that we are likely to see as payment for database queries and news bytes.

Chapter Four introduced us to digital security, an area that is very important due to the inherent insecurity of TCP/IP, the Internet protocol. The most developed systems make use of highly complex and secure transport methods to almost guarantee the safety of any information that is being transmitted.

A cash based scheme, such as CAFE or Mondex, offers a multi-level payment system consisting of the ability to use cash in places other than Internet shopping centres. These systems that require no central processing or authentication introduce a cost-efficient way to do business. The no-overhead cost allows for purchases to be made for any value from a fraction of one penny to millions of Pounds. The cards

also have inbuilt security features that are completely independent of the transmission method that is used.

Token based schemes such as NetCash and DigiCash require customers to purchase electronic currency certificates through an account established in advance. Once issued, the electronic currency represents value and may be spent with merchants who deposit the certificates in their own accounts or spend the money elsewhere. A token based mechanism requires central processing. One issue, apart from the cost effectiveness of low value transactions is that of the issuer having a bottleneck of transactions to clear. This is analogous to getting a credit card verified by an issuer on Christmas Eve, it is notoriously hard to do. The principal disadvantage of token systems is the need to maintain a large database of past transactions to prevent double spending.

CHAPTER SIX

PAYMENT SYSTEM REQUIREMENTS

This chapter aims to map out the key user requirements for an Internet payment mechanism .

It is structured by looking at the subject mostly from the viewpoint of a system's users, not the financial regulators or the currency issuers. This should ensure that it is not only the technical matters that are discussed. However, an article published in New Scientist magazine by A. Lawrence [ALA] stated that 'a secure payment mechanism is an essential requisite for the effective expansion of the Internet marketplace'. Security is therefore taken as the first issue, before looking at commercial requirements and constraints.

The requirements above were gained from talking with representatives of various financial establishments, including NatWest and Fidelity International, by reading company documentation such as First Virtual's and by talking to friends and colleagues.

6.1 SECURITY REQUIREMENTS

Whilst firewalls serve a valuable purpose in securing Internet connected networks, they do not provide end-to-end transaction security and they cannot therefore be considered an adequate security solution for every day financial Internet transactions. A robust security solution for transaction processing should satisfy the following fundamental requirements.

From a consumers point of view, a transaction should be:

Trustworthy
Safe
Anonymous

6.1.1 Trustworthiness

Trustworthiness would ensure that a consumer is able to rely on the second party in the transaction as well as the transport mechanism itself. Network availability is not included in this, as it is an uncontrollable factor.

The ramp-up of on-line businesses will lead to an extensive global marketplace. Whereas today's consumers are used to dealing on buying products from local and occasionally national retailers, tomorrow's consumers could be ordering products from anywhere in the world. If this is combined with the possibility of many Small to Medium Enterprises entering the market (the size of the company is transparent to a consumer who is buying on the Internet) then it can be seen that there may be a need for certification of the payee. If this is an issue, it may be necessary to consider trusted intermediaries such as banks to take on the role of certification authorities.

6.1.2 Safety

Consumers will no doubt require cast-iron guarantees that they can make or receive payments safe in the knowledge that a third party will not re-direct funds or impersonate a user in order to steal cash and/or goods.

However, the second best way that safety can be assured is to send any critical details over a different medium, which severely reduces the risk of interception. Technology and science have now advanced enough to allow encryption and digital signatures to become an integral part of electronic commerce. Encryption techniques ensure that any data intercepted could not be read if a message were intercepted.

6.1.3 Anonymity

Digital cash users should be anonymous in their dealings. Each individual transaction should only be known by two parties - the buyer and the seller.

Anonymity can be completely assured by removing any information about the identity of a consumer in the payment mechanism. This poses obvious problems if we were to look at mechanisms that third parties are involved in, or where checking the identity of the buyer is an integral part of the payment process. As in safety (above), encryption techniques are now available that can be used to remove the opportunity for hackers to penetrate a message, and digital signatures provide a means of confirming the validity of a user without necessarily divulging the identity of the consumer.

On other aspect originating from this view is that consumers should also have the option to remain completely invisible to the existence of a payment on their behalf.

6.2 COMMERCIAL REQUIREMENTS

Any Internet Electronic commerce user could expect the following in addition to the security aspects discussed previously:

Ease Of Use
Flexibility and Off-line Capability
Universality
Expirability
Cost Effectiveness
Reusability

6.2.1 Ease of Use

Digital cash should be easy to use from both the customers and the retailers point of view. The process should require no more thought than spending real money. Matonis [MAT] states that 'simplicity leads to mass use and mass use leads to wide acceptability'.

6.2.2 Flexibility and Off-line Capability

There should also be requirements that allow payment to be made to a retailer without any necessary interaction needed with a third party. Reflecting the usage of cash, availability must be completely unrestricted, with all transactions between the two parties being off-line.

6.2.3 Universality

Thirdly, use of digital cash should not be subject to dependency on being in a certain location, for instance being on a unique computer network. The payment mechanism must be able to be used on a wide basis such as in shops and restaurants. As Matonis said, "this is primarily a brand issue, as it implies recognition of and trust in the issuer".

6.2.4 Expirability

It is imperative that digital cash does not expire. Otherwise this could lead to a crisis in confidence of the issuers. The cash must hold its value until it is either lost or mislaid. Like cash, it should be able to be stored for a while, and retrieved many years later for use.

6.2.5 Cost Effectiveness

Many shops and companies impose a minimum transaction fee when using credit or debit cards. This is to ensure that the transaction fee of the card provider is serviced in the transaction amount. With digital cash we must ensure that there is no additional transaction fee, implying that there will be no lower limit to the value of a given transaction. Flohr [FLO] similarly states that a currency must have 'divisibility' to make high volume, small value transactions practical.

6.2.6 Reusability

This is the ability to re-use digital funds received to make other payments without having to change or update the funds at a 'bank'. This essentially means that peer to peer transactions are possible without the need of a digital currency issuer.

6.3 CONSTRAINTS

In the attributes above, both commercial and security concerns have been raised. However, additional consideration should be aimed at the final part of the transaction, the communication between a retailer and the payment issuer. When looking at an Internet payment system the following should be noted.

Acceptability
Integration
Non-Exclusivity

6.3.1 Acceptability

Small retailers will want to ensure that they are not forced to use a payment mechanism that is unacceptable in the everyday market. Therefore a payment mechanism should aim to provide a universal service, potentially excepting no-one from the system that wants to use it.

6.3.2 Integration

Integration is a major issue. It will not be plausible for a merchant to install many hardware and software combinations just to accept a new payment method. Therefore a payment mechanism must aim to integrate with existing systems software and hardware. This feat may not be easy but if implemented, is certain to have a positive knock-on effect on the acceptability of the scheme. It is also important to note that the great majority of merchants will want to ensure that any Internet payment schemes can be easily integrated into existing payment mechanisms. Credit and debit card issuers will also have this as a concern as they have their market share to protect.

6.3.3 Non-Exclusivity

Integrating the above two points creates a small obstacle. Independent traders and small companies will not want to be excluded from the Internet by the widespread use of a payment system that is only available to people participating in a particular consortium.

6.4 SUMMARY

A system should aim to meet the following requirements:

SECURITY	COMMERCIAL	CONSTRAINTS
Trustworthiness	Ease of Use	Acceptability
Safety	Flexibility	Integration
Anonymity	Universality	Non Exclusivity
	Expirability	
	Cost Effectiveness	
	Reusability	

Table 2: Summary of Payment System Requirements

To clarify the important points and issues a ranking order could be established that would give precedence to more important issues. After much deliberation it is believed that there is no sound basis to this idea. For example, anonymity is more important to some people than others and is a benefit in some situations whereas it may be a hindrance in others. To put this in perspective, we can look at the current situation regarding cash and credit cards. Cash is wholly anonymous (assuming that serial numbers are not traced). Many people prefer to use credit cards, which are accountable and traceable systems. This shows that the general public are generally not concerned whether a system is anonymous or not.

Anonymity may be difficult for users of electronic commerce despite the obvious benefits. Many parties do indeed want the option of having anonymous transactions without it being a necessity. The challenge is perhaps to provide assurances to the payee that the payment is authentic, and to provide the payer with a receipt that produces irrefutable proof that the payment was made.

Some of the findings have and can not been included as they fall outside the project scope. One example of this is that consumers would ideally like some form of consumer protection. Caveat Emptor (buyer beware) legislation is inapplicable on international networks.

CHAPTER SEVEN

MECHANISMS VERSUS REQUIREMENTS

This chapter describes what each payment mechanism offers in relation to the requirements suggested in the previous chapter. The essential differences can be seen in the accompanying tables, and initial glances suggest that a cash mechanism based electronic commerce system is best as it fulfils all the commercial requirements. However, this may not be the case for the further requirements.

7.1 SECURITY REQUIREMENTS

Credit / Debit	Trustworthy	Safe	Anonymous
CURRENT Credit / Debit	×	×	×
First Virtual	✓	✓	×
MasterCard / Visa / Amex	✓	×	×
CyberCash	✓	×	×
BankNet	✓	×	×
Financial Services (FSTC)	✓	×	×

Table 3A: Dissection of Security Requirements - Credit

The basic use of a credit card for payments over the Internet is only as secure as a credit card transaction over the telephone as eavesdroppers are evident on both types of network. As has been previously mentioned, certain electronic payment mechanisms provide encryption facilities to allow authentic private transactions to include credit card details. It is important to realise that the tables only take into account the Internet part of the payment system and not the underlying private networks of Visa, MasterCard or American Express.

After careful thought, it has become evident that a credit card transaction over the Internet is very insecure. Assuming that most users are on a PC platform, it is easy to write a program that runs undetected and monitors the inputs to software by analysing keystrokes and watching for credit card numbers. The reasoning behind this is that there is no possible way of ensuring that all software installed on a machine can be trusted, and it is therefore unwise to trust any 'secure' software because malicious software could have easily been interposed between the user and the trusted software. This can be seen in the following diagram:

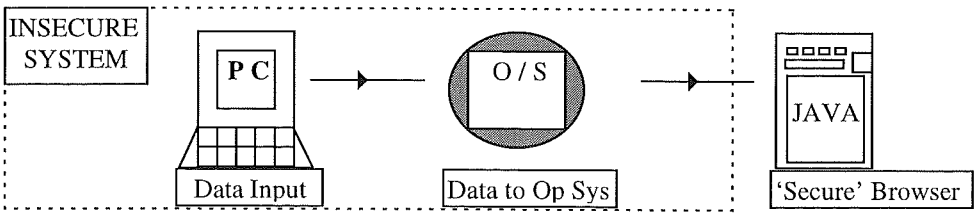


Figure 10: Secure Software Trap

This approach highlights one major issue concerned with electronic commerce. Credit card numbers are very vulnerable to this kind of attack because they have characteristics that make susceptible to fraud.

- Credit card numbers can be easily recognised by pattern recognition. It is known that the last digit, for instance, is always a check digit.
- Credit card numbers have no user level confirmation required for use.
- Credit cards imply that there is virtually always money available.

The attack highlights the fact that credit card encryption software such as that used by CyberCash can be easily undermined, and that secure technology built into web browsers such as Netscape, Mosaic and Java is similarly at risk.

First Virtual is arguably the only system to be totally safe, as the user's credit card details are never placed on the Internet. Instead, the user provides it over the telephone (which IS insecure). Purchases are then made with a 'VirtualPIN', which is essentially an Internet alias for the credit acrd number. There are several added security features which ensure that the system is slightly more secure. These include the use of e-mail to verify a transaction, making the process of stealing numbers difficult to automate as well as using free form text to transmit messages which have no recognisable structure.

There is also no real anonymity in credit and debit based systems as an intermediary is required to verify transactions. Whenever a transaction is made, a trail is left which is ultimately traceable. This detracts from the advantages of being able to use a payment system without actually needing to set up a new bank account.

Cash Mechanism	Trustworthy	Safe	Anonymous
CURRENT Cash	✓	×	✓
Mondex	×	✓	✓
CAFE	×	✓	✓

Table 3B: Dissection of Security Requirements - Cash

The cash payment systems are both safe, due to the ability to lock the card with a PIN number. It is ultimately down to the owner to provide this basic level of security and, of course, PIN numbers can be guessed or stolen. The second 'safe' feature of the cards is that their use throughout their respective systems can be stopped within ten minutes by a phone call to the card centre. Therefore if a card is lost and unlocked, it may still be possible to keep any money that is on the card. Mondex also adds another level of safety by the constant security updates that the cards hold. With the 'cascade' effect, it is possible to update the security on all cards within a very short time span. This is effective, efficient and in the best interests of customers.

Cash is anonymous, and the two cash based mechanisms are untraceable. It may be said that as Mondex provides a log of the last ten transactions then it is not truly anonymous, especially as it leaves an 'ident' on the Mondex card with which the transaction was completed. However, these facts do not make the system traceable for two reasons. Firstly, the user's log is only visible when the PIN is entered into the card and secondly, the ident can literally be anything. There is no need or requirement for a user to put in his name as verification, it is possible to put anything from a surname to six sequential numbers as an ident. It has also been mentioned that no central processing is required and that only the two participants' cards are involved in the transaction, so no central records can be kept or interrogated and hence the anonymity of cash is maintained.

Token Mechanism	Trustworthy	Safe	Anonymous
CURRENT Token	✓	×	✓
DigiCash	×	✓	✓
NetCash	×	×	✓

Table 3C: Dissection of Security Requirements - Token

It may also be noted that as the software for Mondex and CAFE is resident on the smart card and authentication techniques are used it can be deemed that using the cards over an insecure communications channel such as the Internet has no effect on the overall safety. In the token based mechanism the tokens may be 'blinded' to provide anonymity. This is available within DigiCash, but is only necessary when the anonymity is compromised by the need for all transactions to be sent back to the issuing bank for verification, logging and re-conversion from tokens to cash.

7.2 COMMERCIAL REQUIREMENTS

Table 4 shows that all the mechanisms discussed are relatively easy to use, which should prove a major advantage to the general acceptance of electronic cash as a payment system. Having used most of the systems, Mondex appears to be the easiest to use, but most credit and token systems are not far behind. The advantage of having a user-friendly Graphical User Interface is that people become less afraid to use a system., which can only improve the general level of acceptability. The credit/debit mechanisms ease of use is wholly dependent on the implementation of the security mechanism used. The more complex the security, the more time it takes to compute keys and utilise key management. In turn, this may make the use of sophisticated security a hindrance.

The definition of flexibility in Chapter 6 examines the ability of a system to make a transaction without the interaction of a third party. Only a cash-based mechanism achieves this, as systems such as CyberCash or DigiCash require intermediate actions in the form of verification of credit card numbers or token numbers. Only systems based on the cash mechanism discussed in Chapter 3 would ever satisfy this need.

The universality of a system defines the ability of a payment system to be used in a range of different areas. Again, a cash based system has an advantage, as it flexible and requires no verification, whereas a credit/debit based system utilises intermediate actions to complete a transaction. The token model limits its availability to the Internet. When we talk about true electronic cash, we want be able to make payments over other networks, such as cable or satellite television.

	Credit / Debit	Cash Mechanism	Token Mechanism
Ease of Use	✓ (α)	✓	✓
Flexibility	× (β)	✓	× (β)
Universality	× (χ)	✓	× (δ)
Expirability	× (ε)	✓	✓
Cost Effectiveness	× (ϕ)	✓	× (ϕ)
Reusability	× (γ)	✓	× (γ)

Table 4: Commercial Requirements

Key to symbols used in Table 4:

(α) wholly dependent on implementation of security mechanism
(β) requires intermediate actions
(χ) No peer to peer transactions
(δ) DigiCash only available on the Internet
(ε) Expire when banked
(ϕ) Costs are associated with central transaction processing
(γ) Cannot be respent without being banked

When compared, it can be seen that the option has been taken to put token systems as a mechanism that like cash, does not expire whereas credit/debit systems generally do. The reasoning behind this is simple: digital cash will hold its value (ignoring inflation) until it used, tokens will similarly hold their value. It is true that tokens expire. However, the token issuers will allow expired tokens to be exchanged for new tokens. One disadvantage of this is that electronic cash held in lieu of physical cash does not earn interest. Credit/debit mechanisms do not actually hold any currency, as it is a post-paid model. It is for this simple reason that the system is not classed as expirable.

The cost-effectiveness of a payment mechanism is directly related to the overheads required to make a transaction. In other words, the less interaction that is needed for credit checking, verification and error checking, the more cost-effective a payment network can be. To ensure that 'micropayments' are available, each payment model must provide a low cost network. Unfortunately, the credit and the token models both require an intermediary which immediately adds cost to any given transaction. The cash

model, with no intermediary, implies that the channel is a good way to make small payments, although this remains to be seen in practice.

The final commercial requirement from the previous chapter is reusability. This is quite similar to flexibility as it requires that the user be able to continue to use the currency without the interaction of the service provider. Peer to peer transactions are part of most physical transactions, so currency implementors must try to add this functionality into their payment mechanisms. The only systems that allow this are the cash systems, including Mondex, which allow money to be transferred from one card directly to another. Both the credit/debit and token systems allow the cash to be respent, but only after it is banked.

7.3 CONSTRAINTS

	Credit / Debit	Cash Mechanism	Token Mechanism
Acceptability	×	✓	✓
Integration	✓	✓	×
Non Exclusivity	×	✓	✓

Table 5: Constraints of Payment Systems

The above table represents the payment models versus the possible constraints of a new payment mechanism.

Acceptability is arguably the most important issue. Currently there are credit/debit and cash based mechanisms in use world-wide and outside of the Internet and other open systems. This therefore means that their use on the Internet should be easily integrated into current banking practice. As token mechanisms are a new idea and not subject to everyday consumer usage, they can not easily be accepted by consumers or integrated into a system without them being converted into a different method of use, that potentially makes the consumer believe that they are using a different method of payment. Consumers are receptive to some 'token' ideas, such as phonecards and gas pre-payment cards and it is not therefore impossible to get them to use new methods.

The negative mark given to the credit/debit mechanism is given because of the need for a merchant to gain an authorised status to accept credit cards. This implies that some merchants can be excepted from the system and it is therefore not widely acceptable. We must also be aware that credit systems are not always available to small merchants or sole traders due to cost effectiveness of dealing with consistent small value transactions.

Integration is a major issue. It is not plausible to expect a merchant to have x amount of software packages to accept y different payment schemes. The software must be able to integrate with any existing hardware and software, and could be highly beneficial if linked with stock control systems or customer information databases. Two of the three payment mechanisms can be easily integrated with exiting packages and can run concurrently with existing payment systems such as credit card details taken over the telephone. However, token based payment systems are more suited to purchasing information rather than goods and therefore cannot be expected to integrate easily with stock control systems, as there are none.

The sum of acceptability and integration is that of non-exclusivity. On one hand retailers will not want to be excluded by the widespread use of a payment system, on the other hand they will want to use a system that integrates well with current financial instruments. Both cash and token are not exclusive, but as credit and payment networks are legacy systems generally, they are not able to be easily integrated with other payment methods.

7.4 SUMMARY

After examining the tables it is evident that the biggest problems with credit/debit based systems are the failure to provide anonymity and the failure to provide truly secure software. While the anonymity can be improved by the use of blinding, the only way to solve the safety problem is to employ the method used by DigiCash, which requires card details to be given over the telephone. Anonymity is available in all electronic token and cash based systems.

The commercial requirements are easily satisfied by the cash based mechanisms, which severely outflanks both the credit/debit and token models. The main issue regarding the commercial requirements and credit cards is that the credit companies have strict guidelines regarding who can be a merchant and who can use the systems to verify transactions. With a network already in place, the flexibility and universality of the network is highly questionable and the effect that central transaction processing has ensures that the reusability and expirability are not issues that can be resolved easily.

Tokens appear to be midway between the cash and the credit/debit concepts. While it is truly easy to use and like cash, the tokens never expire, it still has problems with universality and flexibility for the same reasons as credit cards.

It can be seen that like our commercial requirements, the cash-based system scores positively against the constraints. It has been argued that to be plausible as a payment system, electronic cash must be acceptable and easily integrated and unfortunately, neither the token based models or the credit/debit based protocols fulfil the requirements.

Overall the requirements show that a cash based commerce system can serve as the basis for an electronic cash system. However, just as cash has a universality within a defined boundary (e.g. legal tender within national borders) digital cash will have boundaries defined by either the political or commercial imposition of 'borders' or implicitly defined by the currency which is being transacted, be they CyberDollars or CyberDeutschMarks.

CHAPTER EIGHT

A CREDIT BASED SYSTEM: CYBERCASH

The following three chapters take an in-depth look at systems representing the credit/debit, cash and token models respectively. They were chosen as 'best in class' systems that, after careful research, provide superior facilities and functionality above their competitors in their respective markets.

Each in-depth study includes an introduction, sample transactions and other important information about the systems. Throughout the reports the products are evaluated to provide an insight that is not available from the on-line brochures that are distributed by the payment companies involved. The evaluations given are in-depth system evaluations as opposed to a direct copy of the general model evaluations given in Chapter 7.

This chapter studies the CyberCash system, whilst Chapter 9 researches Mondex and Chapter 10 looks at DigiCash.

8.1 INTRODUCTION

Like most electronic payment systems CyberCash is designed to make it easy to pay for services and goods with a Web browser. The system relies heavily on encryption and digital signatures designed by RSA Data Security Inc. [RSA] and is designed to run on Microsoft Windows, Macintosh and UNIX systems. Of all the payment mechanisms mentioned in this project, this system must be singled as it is the only software program that is freely exportable in its original state, including algorithms. CyberCash states that it convinced the United States government that the software cannot be used to exchange anything other that CyberCash payments. This is a very strong feature.

CyberCash's Secure Internet Payment Service enables merchants to provide their customers with an on-line payment mechanism that is both viable and secure. This is done by imitating the current Point-of-Sale systems, but replacing the credit or debit 'swipe' with CyberCash. Fees for each transaction are strongly related to fees for existing point-of-sale systems.

The CyberCash software acts as a front end to any of the retailers current systems. This will often include links to banks and payment processors.

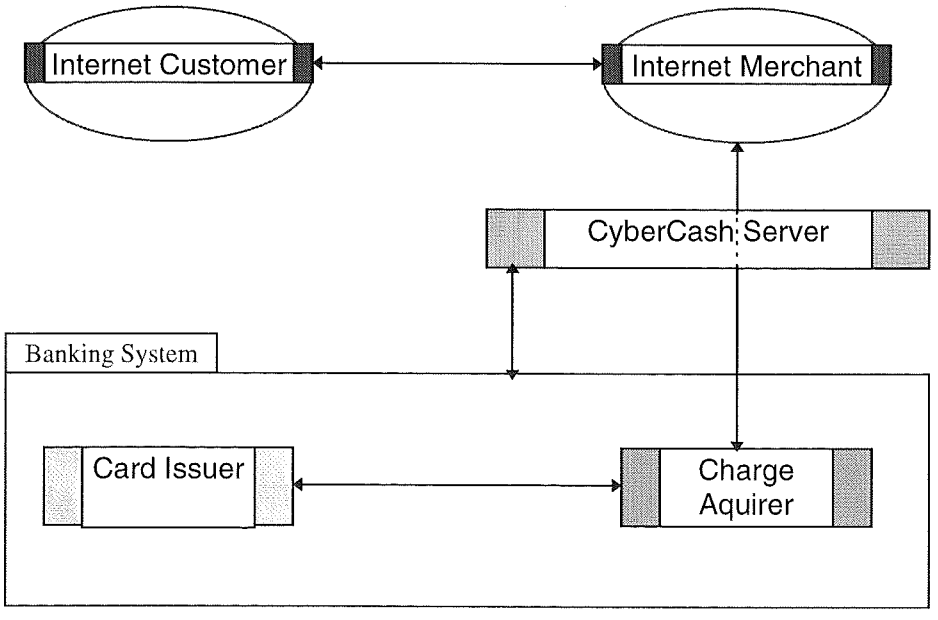


Figure 11: CyberCash System Overview

8.2 WHAT CYBERCASH PROVIDES

CyberCash consists of three pieces of software:

- CyberCash Wallet
- Secure Merchant Payment System (SMPS)
- CyberCash Gateway Servers to external financial networks.

The CyberCash wallet is a piece of software that is available free of charge from the CyberCash web site. It is also available from many ftp sites and is distributed by many Internet Service Providers including CompuServe. CyberCash claims that this makes it a universally available payment mechanism though at the moment this is debatable.

The Universality of the software means that for merchants registered with CyberCash that there is a pool of consumers ready and willing to purchase goods and services over the Internet.

Once the software is downloaded and installed, the CyberCash wallet can connect to merchant web sites. The installation process helps the consumer to get a CyberCash WalletID and then links a credit card number to this public key for authentication. One point to make out is that the credit card number is never stored by anyone except the consumer. The merchant will never store the details and nor will CyberCash. Following this the CyberCash wallet presents a choice of ways to pay. At the moment this is severely limited - to credit cards only. However, CyberCash aim to have the use of debit cards and electronic cheques available in the near future. To actually commit the payment, the consumer clicks the 'PAY' button displayed on a merchant's Web page. This enables the CyberCash wallet to be automatically 'opened', and the money committed.

SMPS is CyberCash's second major piece of software. Distributed to merchants by banks or from CyberCash's Web site, it resides on the merchants Web Server and interfaces with the CyberCash Wallet (mentioned above) and with CyberCash's Gateway servers. SMPS provides the system with which to authorise payments, refunds and providing receipts. In my opinion the software is very strong as it combines secure card processing with administrative functions for the merchant. These include transaction status checking, database interfacing and manual card processing.

Third and finally, CyberCash has Gateway servers that make a secure link between consumers on the Internet and bank's financial networks. The banks receive transactions in the same way as normal credit/debit card transactions, and to all intents and purposes they ARE the same. The Gateway servers provide other services as well as network-to-network translation They also provide the means to maintain and authenticate the CyberCash wallet ID's.

8.3 HOW CYBERCASH WORKS

8.3.1 A Sample CyberCash Transaction.

1. A CyberCash merchant is visited. The consumer wants to buy a product. The price is agreed.
2. Addresses and final price are agreed upon and exchanged.
3. The Web server displays the PAY button. This initiates the transaction.
4. The consumer clicks on the PAY button. The Web server sends an electronic invoice.
5. The consumers CyberCash wallet automatically opens. Payment method is selected.
6. An encrypted payment message is sent to the merchant's web server.
7. SMPS receives the payment message and adds the merchants ID information.
8. This is forwarded to the gateway server and then on to the bank.
9. The gateway server decrypts the message and authenticates the consumer and the merchant.
10. A message is sent to the bank requesting charge approval to the payment method.
11. <bank response> is sent to merchants Web server and on to customer.
12. A positive response means the merchant gets a digital receipt.
13. A negative response means the customer can select an alternative payment method.
14. The merchants Web server sends the consumer a digital receipt.
15. The merchant delivers the goods.

A typical transaction should take less than 20 seconds (source: CyberCash). CyberCash effectively acts as a certificate granting authority by issuing public-key pairs to users. This implies that packets are smaller since the consumers and merchants do not add a certificate to each packet, and therefore transaction times are less.

The major concern is that one effect of issuing public key pairs is that the whole system becomes proprietary. The system is closed because it is nearly impossible for several CyberCash clearing centres to work in the same way as, for instance, there are competitive clearing systems for MasterCard and Visa. This is not because of the public-keys, as it is not a major problem giving competing CyberCash clearing centres access to public-keys, but there may be problems distributing the correct public-key of each merchants CyberCash clearing account to all known customers.

The system is easy to use and the merchant software is very flexible. Each transaction can be made and funds transferred while the consumer is on-line. Alternatively, a transaction can be delayed for any period of time. The system also allows for voids and refunds.

Each CyberCash wallet contains full details of each transaction in a special log. Each merchant system also contains a database logging all transactions and systems actions contained within the SMPS.

In addition, the bank can be queried for additional information. For security, the records kept in its database are encrypted and are only made available (via a password) in the event of a refund. This means added protection if the web server security was ever compromised, yet emphasises the lack of anonymity.

8.3.2 Security and Authentication

CyberCash payments are protected by an encryption system combining DES private-key and RSA public-key software. As mentioned in the first paragraph, CyberCash is unique in the fact that it has United States government agreement to export a product containing 1024 bit RSA and 56 bit DES encryption. These are "hard" cryptographic solutions that offer industrial strength security for payment transactions. Although this is not an impossible encryption algorithm to crack, it would take a multitude of supercomputers to complete the task as the key would be over 100 hex digits.

The CyberCash user interface asks for a consumer to specify a short name or word as an Identity for the user. CyberCash then adds check digits to the requested WalletID to minimise the chance of accidental ID selection. Possession of just a WalletID without the private-key is of no effect. The CyberCash system does have an emergency provision in place that associates an emergency passphrase to a WalletID. When CyberCash receives this ID they will suspend activity on the account, providing a degree of protection against misappropriation to the user.

Packets that move between the Wallet, the merchant and the gateway are encrypted with the 56 Bit DES key. This key is then encrypted by the 1024 bit RSA key and added to the end of the DES encrypted message. This means that the merchant can never learn the credit card number unless the bank chooses to release the information. The merchant's Web server, as stated above, maintains no permanent storage of card numbers.

8.4 CYBERCASH IN DETAIL

CyberCash passes five different kinds of messages between clients and the CyberCash system [EAS]. These are:

- Registration of a new CyberCash ID
- Credit Card binding
- Consumer Purchase details
- Merchant Purchase details
- Utility Messages

These five messages are consistent in structure, consisting of tags and a checksum. All the important details such as Credit Card numbers are sealed inside the message by the aforementioned RSA algorithm. The following example shows an initial message sent to create a new CyberCash user [EAS]:

```
##########################################################################
Sender: CyberApp
Receiver: CyberServer
##########################################################################
Sample Message:

$$-CyberCash-0.8-$$
transaction: 123123213
date: 19950121100505.nnn
cyberkey: CC1001
opaque:

FrYOQrD16lEfrvkrqGWkajM1IZOsLbcouB43A4HzIpV3/EBQM5WzkRJGzYPM1r3noBUc
 MJ4zvpG0xlroY1de6DccwO9j/0aAZgDi9bcQWV4PFLjsN604j3qxWdYn9evIGQGbqGjF
 vn1qI1Ckrz/4/eT1oRkBBILbrWsuwTltFd84plvTy+bo5WE3WnhVKsCUJAlkKpXMaX73
 JRPoOEVQ3YEmhmD8itutafqvC90atX7ErkfUGDNqcB9iViRQ7HSvGDnKwaihRyfirkgN
+lhOg6xSEw2AmYlNiFL5d/Us9eNG8cZM5peTow==
$$-CyberCash-End-kchfiZ5WAUlpk1/v1ogwuQ==-$$
```

Figure 12: Initial Request

It can be seen that the start and the end of the message are shown by the tags beginning and ending with double dollar signs. The extra alphanumeric contained in the last tag is the checksum to ensure that the message has not been corrupted during transmission. It must be noted that the transaction number is generated randomly by the client and is used later on to identify the transaction in other communications.

The opaque (below) contains the DES encoded information with a session key that is encrypted with one of the public-keys. The particular key is identified by the cyberkey tag. This is where the 1024-bit RSA encryption is used. The opaque section of the message contains the following:

8.4.1 Opaque Section Contents

```
type: registration
swversion: 0.8win
content-language: en-us
requested-id: MyRequestedCCID
mail: myemail@myemailhost.com
pubkey:
 0VdP1eAUZRrqt3Rlg460Go/TTs4gZYZ+mvI7OlS3l08BVeoms8nELqL1RG1pVYdDrTsX
 E5L+wcGCLEo5+XU5zTKkdRUnGRW4ratrqtcte7e94F+4gkCN06GlzM/Hux94
signature:
 v6JGmxIwRiB6iXUK7XAIiHZRQsZwkbLV0L0OpVEvan9l59hVJ3nia/cZc/r5arkLIYEU
 dw6Uj/R4Z7ZdqO/fZZHldpd9+XPaqNHw/y8Arih6VbwrO5pKerLQfuuPbIom
```

Figure 13: A Registration Request

The opaque obviously contains the e-mail address of the new person and the public-key that they would like to use. The signature field contains a digital signature of every field in the message (including the unencrypted data such as the transaction number). There are three possible responses to this system, two of which are error messages that are used to update the software package when it is an old version and the third is to include an official CyberCash ID for future use and confirm other given details.

To allow CyberCash to block certain types of incompatible credit cards, users must *bind* their cards, effectively pre-registering them to save typing in the numbers repeatedly. The messages contain all of the card details that are used when a transaction occurs and a special feature known as the card *salt*. The salt is an extra packet that is hashed with the card number. To make the server files a bit more secure, the server does not hold the credit card number, it just stores the hash. This means that when a transaction takes place, the consumers software sends only the hashed credit card number along with the salt.

8.4.2 Transactions

An example of a transaction can be seen on the following page.

The diagram shows that there are tags containing information relating to cost, credit cards accepted, total price and an order identifier, as well as others. The user's computer will decode this and display the information in a more manageable form. The client computer will also ensure that the list of credit card payment options are only the options bound to the CyberCash ID. The user can then choose the payment method from this list.

As the user does not know the merchants public-key, the merchant-signed-hash field cannot be used by the customers CyberCash software. It appears that CyberCash has chosen not to allow its certificate-granting powers at this level. The effect of this is that if a merchant backs out of an agreed transaction then the customer could not verify that an offer of price was agreed. This is not a major problem as most transactions are for the purchase of a fixed price object, however it may lead to concern when people are purchasing services, and a guaranteed estimate is needed.

```
$$-CyberCash-0.8-$$
type: payment-request
merchant-ccid: ACME-012
merchant-order-id: 1231-3424-234242
merchant-date: 19950121100505.nnn
note;
   ACME Products
   Purchase of 4 pairs "Rocket Shoes" at $39.95 ea.
   Shipping and handling $5.00
   Total Price: 164.80
   Ship to:
           Wily Coyote
           1234 South St.
           Somewhere, VA  12345
merchant-amount: usd 164.80
accepts: visa:CC001, master:CC001,amex:CC001,
       JCPenny:VK005,macy:VK006
url-pay-to: http://www.ACME.com/CybercashPayment
url-cancel: http://www.ACME.com/CyberpaymentCancel
url-success: http://www.ACME.com/ordersuccess
url-fail: http://www.ACME.com/orderfail
merchant-signed-hash: N9MHKQoUj26kNtL2YGMiV9NgfCrux
     1AfYo2YnFs0zscLaURhcZzX/QOHwbXJr9yZzJP+LLvXyFTv
     mavLhzOTzotgcAx+jJA6W++a6mVkwxEbIyORRazBCoG9tiO
     sXdAU
$$-CyberCash-End-1SLzs/vFQ0BXfU98LZNWhQ==-$$
```

Figure 14: An Example of a Payment Request

When a customer accepts a transaction, the client software will generate a message similar to the one below:

```
   $$-CyberCash-0.8-$$
   type: card-payment
   id: myCyberCashID
   order-id: 1231-3424-234242
   merchant-ccid: ACME-012
   transaction: 78784567
   date: 19950121100505.nnn
   pr-hash: c77VU/1umPKH2kpMR2QVKg==
   pr-signed-hash:

a/0meaMHRinNVd8nq/fKsYg5AfTZZUCX0S3gkjAhZTmcrkp6RZvppmDd/P7lboFLFDBh
Ec0oIyxWeHfArb3OtkgXxJ7qe0Gmm/87jG5ClGnpBnw0dY7qcJ6XoGB6WGnD
cyberkey: CC1001
opaque:
 iff/tPf99+Tm5P7s3d61jOWK94nq9/+1jOWK9+vr9+b+94n3tYzmiveJ9/+09/334ubg
 3rWM5Ir3ier3/7WM5Ir36+v35v73ife1jOWK94n3/7T3/ffm5uD+7N339/f39/eq3ff3
 9/eFiJK5tLizsoeSmpW7uLS8/7iio7Wisfv38biio7uyufv3tfv35uH+7N3d9/exuKX3
 5+z3vuu4oqO7srnsvvz8/venoqO0v7al/7iio7WisYy+iv7s3ff3p6KjtL+2pf/wi7nw
 3ard3Q==
$$-CyberCash-End-7Tm/djB05pLIw3JAyy5E7A==-$$
```

Figure 15: Presentation of a Credit Card for Payment.

The opaque section of the message holds details of the transaction as well as a hashed value of the bound card. The merchant is unable to read these details as they are encrypted with the private-key of the user. The only entity that is able to read and decode the opaque is the central transaction computer, due to the fact that it needs to pass details along to the credit card clearing company.

The pr-hash is computed by the client and its authenticity is guaranteed by the signature of the entire message bound inside the opaque block. The pr-signed-hash is a replica of the hashing that the

merchant applied to the original price proposal. The servers decrypt the pr-signed-hash with the merchant's public-key and check to see if it matches pr-hash. If it does, then the deal is agreed by both parties.

The response given to the merchant is bound up in a new message. The original opaque message is unchanged. A new merchant-opaque section is added.

```
$$-CyberCash-0.8-$$
merchant-ccid: ACME-69
merchant-transaction: 123123
merchant-date: 19950121100705.nnn
merchant-cyberkey: CC1001
cyberkey: CC1001
opaque:
 EDD+b9wAfje5f7vscnNTJPkn1Wdi7uG3mHi8MrzLyFC0dj7e0JRjZ2PmjDHuR81kbhqb
 nX/w4uvsoPgwM5UJEW0Rb9pbB39mUFBDLPVgsNwALySeQGso0KyOjMxNs1mSukHd
 OmDV4uZR4HLRRfEhMdX4WmG/2+sbewTYaCMx4tn/+MNDZlJ89Letbz5kupr0ZekQlPix
 +pJsrHzP5YqaMnk5iRBHvwKb5MaxKXGOOef5ms8M5W8lI2d0XPecH4xNBn8BM
 AJ6iSkZmszoQfDeWgga48g2tqlA6ifZGp7daDR81lumtGMCvg==
merchant-opaque:
 6BVEfSlgVCoGh1/0R+g1C143MaA6QLvKpEgde86WWGJWx45bMUZvaAu4LVeqWoYCq
SGfaWKUF7awol0h1i1jtgieyAcXB8ikvRJIsuSAwsRMyoN1ekR6tucvfv/622JY7+n7n
GOGbMzP0GJImh2DmdPaceAxyOB/xOftf6ko0nndnvB+/y2mFjdUGLtFQP/+3bTpZttZXj
j7RO1khe1UrAIk2TGQJmNw+ltsu0f42MgsxB8Q31vjPtoiPi5LEmD0Y4jlpJ7Jg2Ub84
F9vJhYpmzNkdiJUe83Hvo/xfJRbhafJpXFEsUZwQK0jU1ksU6CQd2+CPBB+6MxtsHoxJ
mjD6ickhd+SQZhbRCNerlTiQGhuL4wUAxzGh8aHk2oXjoMpVzWw2EImPu5QaPEc36xgr
mNz8vCovDiuy3tZ42IGArxBweasLPLCbm0Y=
$$-CyberCash-End-7Tm/djB05pLIw3JAyy5E7A==-$$
```

Figure 16: An Authorisation Operation on a Credit Card.

The merchant-opaque section contains this information encrypted with the merchant's private-key. This can be seen below.

```
type: auth-only
order-id: 12313424234242
merchant-amount: usd 10.00
pr-hash: 7Tm/djB05pLIw3JAyy5E7A==
pr-signed-hash:
 a/0meaMHRinNVd8nq/fKsYg5AfTZZUCX0S3gkjAhZTmcrkp6RZvppmDd/P7lboFLFDBh
 Ec0oIyxWeHfArb3OtkgXxJ7qe0Gmm/87jG5ClGnpBnw0dY7qcJ6XoGB6WGnD
id: myCyberCashID
transaction: 78784567
date: 19950121100505.nnn
merchant-signature:
 4qZMe2d7mUXztVdC3ZPMmMgYHlBA7bhR96LSehKP15ylqR/1KwwbBAX8CEqns55UIYY
 GGMwPMGoF+GDPM7GlC6fReQ5wyvV1PnETSVO9/LAyRz0zzRYuyVueOjWDlr5
```

Figure 17: Authorisation by Merchant

The next step for the CyberCash computer is to decrypt the two opaque sections and then verify that the amounts and digital signatures match. If these are correct then the information is forwarded to the credit card clearing house. This elicits a response from the clearing house, stating whether the transaction is authorised. The result is then passed on to the user

The response contains a varied amount of data, with information included for both the user and the merchant. The users message is encrypted with the session-key that the client used to encrypt the credit card data that is sued in the original opaque section. The merchant information is encrypted with the session-key that the merchants server used to encrypt the merchant-opaque data.

The full information about the credit card is not necessarily sent back in the return receipt. CyberCash have not yet decided whether or not to include full details or just the hash key and the card expiration date.

8.5 EVALUATION OF CYBERCASH

So, how does CyberCash meet the criteria that were set in Chapter 6?

CyberCash is a very powerful electronic cash system that successfully simulates the everyday banking system. With full backing for world-wide distribution by the US government, it has a strong head start against its competitors in the race for global dominance.

Security Requirements:
Trustworthy : Safety : Anonymity

CyberCash is both trustworthy and safe. It uses a combination of the most successful and powerful cryptographic software available to ensure that consumers money is safe and that a third party cannot redirect funds. If there was ever a problem, the credit card issuers in the United Kingdom must cover any loss over £50.

There is no real form of anonymity within CyberCash, as the company is able to disclose information to merchants and banks if they request it. Peter Wayner [WAY] believes that the system will offer no greater anonymity than the current credit and debit card networks.

Messages between the three main pieces of software discussed in section 8.2 are all encrypted using 56-bit DES encryption. If this is not enough, the DES key is encrypted using the RSA algorithm and then appended to the already encrypted message. CyberCash also makes use of digital signatures to verify that the sender of the messages is authentic. Overall, the anonymity is totally secure on this part of the payment. Due to reasons cited in Chapter 7, it is evident that this payment method is insecure. When compared to its competitors, it is evident that the part of the transaction that it has authority over is very secure and very hard to compromise.

Commercial Requirements:
Ease of Use : Flexibility : Universality : Expirability : Cost Effectiveness : Reusability

CyberCash meets only one of our commercial requirements and that is its ease of use. When a user wishes to buy an item, they are presented with a straightforward screen detailing the payment cards available. It is extremely user-friendly.

Unfortunately, the remaining commercial requirements are not met. CyberCash is not available off-line and is therefore inflexible. It is also verging on being proprietary due to the company effectively acting as a certificate granting authority with its public key pairs. It is very unlikely that there can be two or more competing CyberCash systems (unlike, for instance, two credit card companies). It therefore does not meet the need to be a universal system. Due to the inherent fee charged by credit card companies, this system cannot be used for small payments. However, if CyberCash started to accept debit cards then this may change, as historically the costs associated with debit cards are lower than those of credit cards. Finally reusability is not an issue. As the currency expires when it is banked, there is no way that it can be reused.

The CyberCash system will be expanded to cope with micro-payments so that people can use electronic cheques or its form of electronic cash. This may lead top overheads being brought down, as more transactions will take place using debit transactions rather than credit.

One final issue with CyberCash is that it supports operations around-the-clock, with no need for any human interaction. This can be regarded as a very visible benefit.

Constraints:
Acceptability : Integration : Non-exclusivity

Integration is the major advantage of a credit based system such as CyberCash. It has been designed to strengthen the current credit card system and this approach is therefore bound to be popular with large retailers who would want to integrate a mechanism with their existing Electronic Point Of Sale (EPOS) systems. Unfortunately, this aspect implies that non-exclusivity is a problem. Small independent traders will be wary of being excluded from an Internet payment system that is only available to companies large enough to be in consortium. CyberCash, as a global payment mechanism, may not be able to juggle small business needs with the requirements of large corporations. Indeed, small retailers may be left out of this and forced to use a payment mechanism that is unacceptable in the everyday market.

The CyberCash wallet is free and works easily with most Web browsers, and can easily be downloaded as and when needed. The fact that a user can decided to use it at any time is a major advantage and means that there no relationship is required for the merchant and user before a transaction can take place.

8.6 SUMMARY

CyberCash provides a system that provides an efficient way with which to carry out on-line transactions. The security within the system is first class and provides a convenient and trustable payment environment that is unique in having their encryption methods licensed by the United States government for export.

The use of credit cards as a payment system also provides CyberCash and its merchants the ability to have a ready-made customer base, which can choose as and when to use a payment system, rather than having to pre-register or use pre-paid tokens.

The system is a positive step towards true electronic cash, although it falls short by resisting the temptation to change some of the disadvantages of the payment method. Instead it piggybacks an existing payment method on to its architecture which just extends the problems associated with credit cards such as guessable number structure.

CHAPTER NINE

A CASH BASED SYSTEM: MONDEX

9.1 INTRODUCTION

Mondex was founded in 1990 by NatWest Bank [NWB] and Midland Bank [MLB]. It is a payment system that combines features of traditional cash with the convenience of global electronic payment. Unlike CyberCash, the main constituent of Mondex is a chip embedded in a credit card-sized plastic card, which digitally stores the electronic equivalent of cash in up to five separate currencies.

Mondex users are able to get cash from anywhere that has either an ATM (Automated Teller Machine), a telephone or a personal computer with a modem. Therefore it is a very accessible mechanism to use. It is also possible to transfer Mondex cash from one user to another using these methods, as well as by using a specially designed Mondex wallet.

Tim Jones, the inventor of Mondex, states that 'Mondex functionality overlaps with cash to the extent that it provides a secure store of value that is divisible, universally transferable and receives widespread acceptance. Cash remains distinct in that it embodies the asset and does not require a silicon chip and plastic card platform for its operation. Mondex is also distinct from cash in that 'virtual' or 'electronic' transfers of value are possible across any computer or telephonic network' [TJH].

Unlike all other payment mechanisms studied in this report, Mondex is a real-time system that allows users to credit and debit money from one account to another without needing to be cleared by a central authority. Its anonymity lies in the fact that no central records are kept of each transaction, although a log of the last ten transactions is kept on each wallet.

The following diagram shows the information flows between user and the merchant, and is directly comparable to Figure 3. The dotted lines represent the banking flows which are not a part of the main transaction.

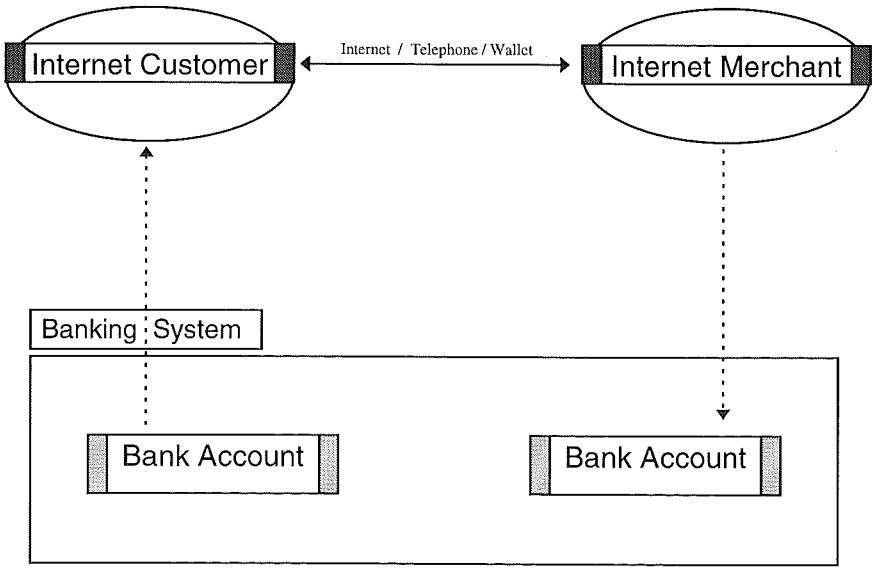


Figure 18: Mondex System Overview

9.2 HOW MONDEX WORKS

As a 'means of exchange' scheme with no clearing and immediate settlement, Mondex allows for the free movement of money. There are three methods which users can transfer cash between the cards.

- In Person
- By Telephone
- By Network

In Person. There are a number of major manufacturers, including Hitachi and Panasonic, who have produced special handheld electronic wallets. The wallets contain a Mondex chip, allowing users to transfer cash between their wallet and their Mondex card. It also allows users to perform various other functions including checking the balance of a particular card and transferring money to other peoples Mondex cards.

One major benefit of the wallet is the ability to use it as a bank to store the majority of cash, and then using the card to store small amounts of cash that may be needed when shopping.

By Telephone. To use Mondex over the telephone, it is necessary to have a Mondex compliant telephone. In the UK these are manufactured by British Telecom. The user can use the telephone line to transfer cash to and from a bank, a merchant or any other party with a Mondex device. The telephones can also be used to check balances and perform other functions.

By Network. Having reached the on-line service or mall that accepts Mondex, the user selects the goods or services that they are interested in. On completion of the selection the Mondex card will be put into a card reader attached to the computer. On confirmation that another valid Mondex device exists at the other end of the link, the value will be transferred from the user's card to the merchant's device.

The use of a system like this has many implications, the most important of which is the opportunity that Mondex provides for the expansion of business over the Internet. Mondex ensures that Internet merchants have a means of obtaining payment that does not require any form of prior arrangement with customers. This is a very efficient method of business, especially if we note that there are no overheads associated with each transaction.

It appears that Mondex is an easily accessible payment method which suits the nature of this project. The facility to transfer Mondex 'cash' over a variety of media makes the scheme particularly suitable for small value Internet transactions and in particular for the type of transaction where an individual is selling a small piece of information over the Internet and is not accredited as a Visa or MasterCard merchant.

At the time of writing Mondex has not been launched nationally. However, when it is rolled out all a user will need is an account with an issuing bank and a Mondex card. No additional equipment is necessary, although in the context of this project an additional card reader will be needed for Internet commerce.

9.2.1 A Sample Mondex Transaction

1. A Mondex merchant is visited on the Internet. The consumer wants to buy a product. The price is agreed.

2. Addresses and final price are agreed upon and exchanged.

3. The consumer puts the card into a card reader connected to the computer and unlocks the Mondex card with a PIN.

4. The consumer transmits the card details to the merchant.

5. Whilst the transfer is in progress, the merchants ID is visible on the consumers card reader and vice versa.

6. Both Mondex cards log the transfer amount and the ID's.

7. The merchant delivers the goods.

A typical transaction should take less than five seconds (source: Mondex). The user interface ensures that the system is easy to use and appears to have been designed to be convenient and user friendly, with each Mondex interface having no more than six standard features. The symbols are shown below and can be seen to be market and language independent.

Balance Select Purse Currency Lock / Unlock Statement Transfer

Figure 19: Mondex Symbols

The merchant software, although sparse of functionality, is well suited to its job. As well as the basic functions of a card wallet, the merchant software allows basic mathematical functions (such as multiplication and division) to be performed. The only other major difference is that the transaction log may be bigger for a merchants terminal.

An important aspect to note is that value only ever moves between Mondex cards - and can only ever be stored on Mondex cards.

9.3 IN DETAIL

All Mondex cards and devices can be locked by one simple keystroke and unlocked by using a unique 4-digit code which can be changed by the user at any time. It is possible for cards to prevent outgoing payments while still being able to receive incoming payments, meaning that an Internet merchant can lock his Mondex card as a safeguard against theft or unauthorised withdrawal.

After a series of incorrect attempts to unlock the card, or even to try and dissect the chip contained within a Mondex device, the card is effectively 'locked out' and cannot be used without being taken to a Mondex issuing bank where entitlement to use of the card can be established.

We must also note that rather than using a physical signature, the Mondex cards create digital signatures to ensure security throughout the system. By issuing digital signatures, the integrity of the system can be maintained by ensuring that any value transferred can only be acquired by the card for which it is intended.

Mondex system security is divided into two areas - the hardware of the chip that is embedded in the card, and the software which controls the flow of funds between the cards.

The Mondex project was designed with security as the foremost concern, and therefore the chip card has been tailor made to protect a users data from unauthorised disclosure and modification from both physical and logical attacks.

The chip currently used in Mondex is manufactured by Hitachi. It is an 8k EEPROM chip, of which the Mondex software takes up 5k. The security aspect of the software is the Value Transfer Protocol which uses advanced cryptography which is algorithm independent and can be based on either private or public key cryptography. Mondex publicly states that when the technology is efficient, they will use asymmetric algorithms. Asymmetric algorithms are those where the key used to decrypt the message is not the same as the key used to encrypt it i.e. public key cryptography.

The Value Transfer Protocol is called into operation when a transaction is taking place; for example, when the card is used to make a purchase over the Internet and the payment is made via a Mondex terminal.

Placing a card into a card reader initiates a two-step transaction process which inaugurates the transfer of funds and ensures that the correct destination is reached and is not fraudulent.

The following is a typical transaction. This is one level below the abstract view shown in section 9.1.

1. Registration.

   The Mondex card stored in the merchant's terminal validates the information provided by the customers Mondex card. Similarly, the Mondex card being used by the consumer validates the information provided by the merchant.

2. Transfer of Value.

   The merchant's terminal requests payment and transmits the digital signature along with the request for payment. Both cards simultaneously check the authenticity of each others message. The consumer's card verifies the signature and then sends the amount outstanding. Following this, the value is deducted from the consumer's card.

3. Close

   The merchant's Mondex card finally checks the digital signature and, when satisfied that everything is in order, sends the acknowledgement (which is again accompanied by a digital signature).

   Only after the value has been deducted from the consumers card is the same value added to the retailers account. This effectively manages to prevent the possibility of duplication and the unauthorised creation of value. Finally, the digital signature of the merchants card is checked by the consumer's card and if OK, the transaction is complete.

One of the major concerns is that of a link failing, possibly causing a transaction to stall. It appears that if a link fails, be it a communications failure or a power black-out - the protocol will continue to try and complete the transaction by waiting to see if communications or power is restored. If this does not happen then the error is recorded in a log kept on the card. It is important to note that this log is independent of the transaction log that the card keeps.

In addition to this security, Mondex uses two values to ensure that messages passed are unique. By including the unique identifier of each Mondex card and a unique sequence number for each transaction, it can be seen that any attempt to use message details for illicit purposes is ill founded.

9.4 SECURITY ASPECTS

The Mondex approach to cryptography is far sighted. In 1978 when Rivest, Shamir and Adelman invented the RSA algorithm, they stated that it would take a 1 MIP computer approximately seventeen thousand years to crack a 425 bit key. In 1994, Bellcore announced that they had managed to crack a 425-bit key. Mondex appears to have realised that there have been many advances over the years, both in computing power and the efficiency of algorithms used for factoring numbers and that the possibility of similar future growth can not be ruled out.

Mondex allows for new cryptography algorithms and software to be introduced into the system without the need to immediately change users' cards. This is accomplished in the following way;

When issued, each Mondex card contains two different and independent security schemes, of which each comprises at least one cryptographic algorithm or public or private keys (See Step 1, Figure 20). Initially the cards are set to operate on security scheme A, but are able to switch to security system B when called upon to do so.

To switch all the Mondex cards that are in issue, Mondex requires a small number of cards to be issued into the scheme that contain security systems B and C. Whenever one of the new cards completes a transaction with an 'old' card (Step 2), it will automatically trigger it to use the B security system (Step 3) and at the same time instructs the card to pass the message on to all cards with which it transacts.

The system does not provide functionality to allow each card to download the next generation of security software to each other. Rather, Mondex can withdraw the original A and B cards over the genuine lifecycle of a card. Furthermore, switches to security systems D, E and F can be introduced into the Mondex system as and when required.

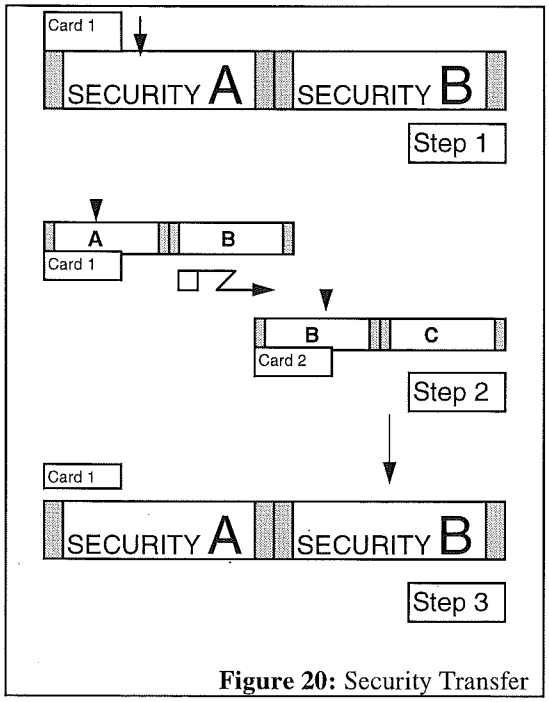


Figure 20: Security Transfer

Exactly how much privacy the Mondex card assures the holder is debatable. By not stating the extent to how much transaction logging the card will allow, the author is led to believe that perhaps anonymity is not a key feature of the system and this therefore affects the security rating.

Academics from the University of Essex have alleged that the Mondex card readers that are used in shops and telephones are capable of recording and storing records of the last five hundred cards as used in the card reader [CLA]. Whether this theory is commutable to a situation regarding card readers attached to PC's is arguable, although it can be seen that any purchase made from a vendor over the Internet may lead to an unauthorised entry on a corporate transactions database. Mondex has claimed that the cards and the transactions are as anonymous as cash.

However, allegations have also been made on Internet mailing lists that the card is designed to download extra information to the issuing bank every time the card is placed in a card reader. There are also suggestions that the systems are programmed to copy the internal error log as well, to ensure that all incomplete transactions are accounted for [GRA].

A major issue is therefore that the system appears to be able to capture and analyse data on trends and unusual situations in a way which is not feasible with suspect physical currency. Every Internet merchant that banks takings provides an opportunity for Mondex to capture transaction data and patterns of behaviour which can be analysed to give warning of suspicious circumstances. For example, because each genuine transaction has a transaction number, any duplication of transaction numbers would indicate potential fraud.

To minimise the criminal opportunity to benefit, the cards generally contain limits to the maximum amount of money that they can transmit in each transaction and a limit to the amount of transactions that can complete before they automatically 'lock out' for review by the issuing bank.

One major issue with the payment system is that experts in the United States appear to have found a way of counterfeiting electronic cash held on smart cards [TIM]. These findings could possible cause a big problem with Mondex's entrance into on-line payments. Scientists at Bellcore [COR] in New Jersey have found that heating a card slightly causes it to give a wrong reading. This has the potential to allow a hacker enough information with which to crack the security that protects the data held by use of brute force methods. This implies that a user has enough mathematical knowledge to do the calculations, which someone undoubtedly will. The levels of security as seen in Mondex are not completely useless. The ability of the data held on a Mondex card to destroy itself if the card is taken apart is a major asset to the system, and will stop 'casual' thieves.

9.5 EVALUATION

It is important to evaluate Mondex against the criteria that were set in Chapter 6.

Mondex is obviously a system that has the potential to go far. It is well thought out, is backed by many multi-national banking corporations and has secured global distribution channels in virtually all major markets.

Security Requirements:
Trustworthy : Safety : Anonymity

> Mondex has been proved to be safe and is arguably anonymous. Fuelled by questions about transaction logging, the anonymity of the system appears to be at doubt. It is true that Mondex deny that this happens, but the fact that Mondex can shut any card out of the system when it is reported lost, implies that there is some way of keeping an eye on cards that are involved with transactions. In this light, we may also say that the card and the system are not trustworthy, but the author believes that this is not the case. The user is definitely able to rely on the mechanism. Evidence of this is reflected in the fact that there is a transaction log to keep a summary of transactions, an error log to show transactions that didn't take place and there is also the ability for a transaction to re-try making contact in the wake of an electricity brown-out or a broken Internet connection. These examples point to almost exemplary trustworthiness for a payment system, and do not take into account the fact that the system is backed by some of the most powerful banks in the world.
>
> Safety and the assurance of transactions is maintained by comparing transaction numbers. Digital signatures ensure that any value transferred can only be acquired by the card for which it is intended. Various crypto-systems are used to deter people from trying to 'steal' the transaction messages.

Commercial Requirements:
Ease of Use : Flexibility : Universality : Expirability : Cost Effectiveness : Reusability

> In effect, Mondex satisfies all the commercial requirements that can be seen above. Its ease of use is evident in the fact that all is required is an understanding of the symbols that can be seen in Figure 18. Arguably, obtaining a card reader detracts from the ease of use when compared to the other payment systems that are being evaluated, but the general user-friendliness is always

apparent. The lack of Internet software availability from Mondex means that there is a long way to go until payments can be successfully made. However, with the graphics designed especially to be globally acceptable, it is evident that Mondex has thought through the requirements of its payment method.

As a 'replacement' for cash, it is also evident that Mondex is completely flexible. The ability to make peer-to-peer transactions provides evidence that access to the system is completely unrestricted. With this in mind, it is apparent that the system is therefore universal, as its usage is not dependent on being on any particular network or in any particular place.

It can be argued that Mondex is expirable, as cards need to be replaced every so often. However, the cash that the chip holds is never lost, and as it is reflective of cash it cannot lose its value. Like cash it can be stored for a while and assuming that Mondex exists in its present form, can be retrieved many years later for use.

By taking these points into account and by remembering that Mondex can make payments for any amount over £0.01, it is evident that Mondex fulfils all the commercial requirements. It must be noted that while there is no overhead cost for a Mondex transaction and while there may be overheads for other payment mechanisms, that Mondex charge a yearly fee to cover their costs, while other payment systems may not.

Constraints:
Acceptability : Integration : Non-Exclusivity

Mondex fares extremely well when faced with the constraints of the system. Mondex is undeniably acceptable, and this is proven in the take-up rate of their trial in Swindon[MON]. By being able to bank takings over the Internet every-day, the reduction in problems regarding the security and banking of physical cash is very high.

Mondex is also easily integrated. By combining desk-to card readers with card-readers for other payment systems or applications, the Merchant has the ability to accept a wide variety of payment methods. As has been stated earlier, Mondex has not released any software yet. As Mondex is suited to both macro- and micro-payments, the ability to integrate the software with both stock control and data-collection programs is a key requirement. It is impossible to say for sure whether or not the software will include this feature.

Non-exclusivity implies that Mondex is available to all. It is, and this is reflected in the wide availability of systems available to suit all major uses. Manufacturers are working on terminals that allow Merchants to participate in many financial consortiums. Of course, the merchant will have to sign up with a bank that has Mondex backing.

9.6 SUMMARY

With relatively little information to analyse, the security architecture of Mondex appears to be extremely robust. As there is only one element to the card - the chip - this means that the card readers required to facilitate electronic commerce over the web do not need to understand how the security or encryption works. In fact, both the transmission medium and the physical devices are only dumb carriers of messages that they need not understand from one Mondex party to another. This implies that the knowledge of Mondex security can be limited to a select few people.

Security is also evident in the fact that with physical money, fraud can take place through the use of normal printing technology to reproduce near-perfect counterfeits. With a smart card the cost of the technology capable of making chip cards can probably be considered economically unviable and then only a perfect forgery will do.

By adding this to both the regular and sporadic cascade updates of the chip and its cryptography process, it is intended that any discovery made by hackers will rapidly become valueless and useless.

Mondex has a large amount of security features and will continue to add to its security with new technology and techniques, both in advance and in response to potential attackers. It is far from perfect especially if the Bellcore research is proved to be correct, but it does provide adequate security in the current electronic commerce environment. If a criminal was to hack the chip, it would not be worth the effort.

The Mondex card is unusual in two respects. First, it is designed to hold five different currencies on one card which is a definite advantage for making payments over a global system such as the Internet; secondly, it allows peer to peer fund transfer without the intervention of a bank or on-line clearing house. These two features are only available with this kind of payment mechanism.

The authors major issue is that it is perhaps too reliant on its tamper resistant technology. If an attacker were to break into the smart card, which is feasibly possible, he would be able to place new money on the card at will. This would create a great deal of non-accounted-for cash. If the system of breaking in was to be widely published, then the issuing bank would be helpless.

CHAPTER TEN

A TOKEN BASED SYSTEM: DIGICASH

10.1 INTRODUCTION

Founded in 1990 by Dr. David Chaum, DigiCash was created to build on Chaum's extensive knowledge of cryptography [CHB, CHC] and to develop and licence competitive payment techniques that display the capability of technology to protect the interests of all participants. One of these competitive payment systems is DigiCash. As discussed in earlier chapters, DigiCash is a token-based system that uses unforgeable packets in place of 'real' money.

According to the on-line brochure, Electronic Cash by DigiCash is 'a new concept in payment systems, combining computerised convenience with security and privacy' [DIG]. This chapter aims to take an in-depth look at the system and to gauge whether or not it is suitable payment system for the future. The amount of information available in the marketplace on DigiCash is negligible. It is therefore necessary to discuss details of the protocol that is available [EPR] and features of the trial system that DigiCash are presently testing.

Like CyberCash, DigiCash is designed to run on the majority of systems. Merchant specific software is required to run on the Windows and Macintosh platforms, although on Unix the text version of the client can also be used as the merchant software.

The following diagram shows information flows based on the DigiCash system. The details are explained throughout this chapter.

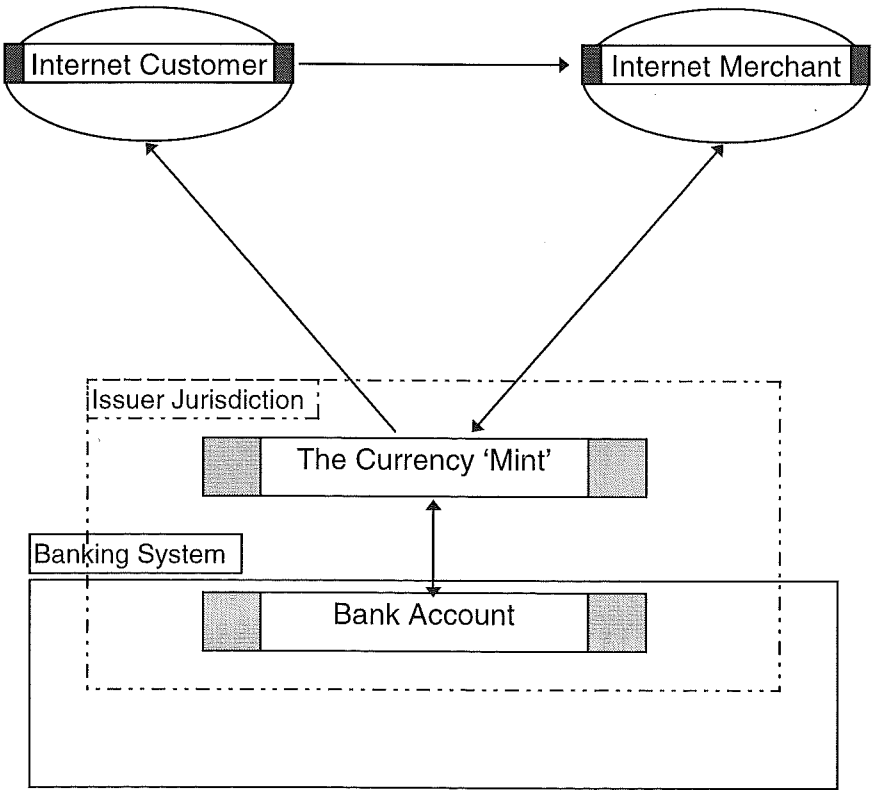


Figure 21: DigiCash System Overview

10.2 HOW DIGICASH WORKS

Ecash is essentially made up of three main constituents that are:

- The Bank
- The Ecash Mint
- The Ecash Wallet

After downloading the software there are three separate places where money can be held. Each user has an account at a bank, which can be an ordinary current account, and may be used for everyday purposes. The second place where money can be is at the Ecash Mint. When the Bank is instructed to transfer money to the Ecash system, the Bank moves the funds to the Ecash Mint. Using the downloaded software it is possible to view amounts held within the Mint, and to transfer the money from the Mint to the Wallet. Once a request has been made for the Mint to produce some coins, these are transferred to the Wallet which is resident on the users hard drive.

The Bank account is where the real-world cash will be held. The strength in leaving cash in a genuine bank account is that it is likely to be insured and likely to earn interest. These are two feats that are not yet plausible in the digital currency arena.

The Mint is the location that provides the validation and certification for money used throughout the Ecash system. It is likely to be filled with the majority of a users digital currency and is relatively secure as it stays resident on the bank's Ecash computer. It is not insured and does not earn interest.

The Ecash Wallet can be filled with token-based coins that are downloaded from the Mint. The coins are bits created with the digital cash algorithm using a blind signature. Like cash, the bits can be lost, misplaced, or stolen. When the user has finished, it is possible and should be recommended to transfer the money back to the Ecash Mint and perhaps back to the Bank account although it is possible to leave the money resident on the disk drive.

The software is available freely from any issuer of the currency. Unfortunately there are only four issuers at present. They are EUNet of Finland [EUN] and three banks, Mark Twain Bank of Missouri [MTB], Deutsche Bank of Germany [DBG] and Advance Bank of Australia [ABA]. Each has its own implementation of the software which is not interchangeable with other versions.

Once the software is downloaded and unpacked, the user is asked to give a password, following which a 768-bit RSA key is produced. Then the user is prompted to download some money from the 'remote' bank to the 'local' wallet.

A DigiCash trial commenced in October 1995 and concluded in April 1996. Although new accounts are not being issued, I was fortunate enough to be allowed to use a trial account that enabled me to test the system [TST]. The currency used in the trial account is called Cyberbucks and has no true value, meaning that it is not exchangeable for a real currency. The account allowed the purchase of information and services from merchants participating in the trial. The account allowed 100 Cyberbucks in a DigiCash bank-account. Although the Cyberbucks were not exchangeable to real money, value was recognised in the goods and services that were available for purchase. Although the software will be different depending on which currency issuer is used, the functionality will be the same throughout and is therefore the basis for the investigation.

10.2.1 Getting Started

To get started with DigiCash, a user contacts the bank and asks for money to be downloaded to the wallet. After entering the RSA secret key, the money is downloaded to the users hard disk as a series of 'coins'. The bank distributes the coins in sizes that grow exponentially.

Therefore £21.00 would theoretically be distributed as:

Number	Value	Amount
8	£0.01	£0.08
8	£0.02	£0.16
9	£0.04	£0.36
9	£0.08	£0.72
9	£0.16	£1.44
9	£0.32	£2.88
8	£0.64	£5.12
8	£1.28	£10.24
	Total:	**£21.00**

Table 6: The Fictional Distribution of £21.00

Smaller coins are included to lower the amount of times that the bank must break a coin to allow change. This is one downfall of the DigiCash system - if a merchant needs to break a coin, the transaction must be interrupted to go to the bank and get change. This makes it very inefficient compared to what can be achieved by a decimal based digital cash system. The system does guarantee a minimum amount of payments that can be paid with each amount of Ecash withdrawn.

Instead of the bank issuing a large amount of coins or a user being required to give change to a merchant, DigiCash use a system that includes an electronic 'check'. This is a number that contains enough denominations to ensure that the right amount is available for a given number of transactions (up to a pre-determined limit). The value of this check is assigned at the time of payment. One effect of having a pre-determined amount of transactions is that it means that users are able to receive interest on their unspent cash, that the bank can receive interest on credit payments, and that the same check can be spent in multiple currencies.

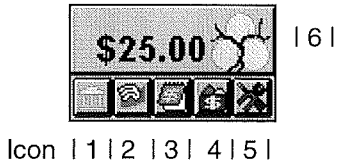
Within Ecash the user's computer generates a random number using a secure algorithm which is used as a 'note'. The user's computer then blinds the note which is transmitted to the bank where it is signed with the private key. The result is returned to the user and the funds are debited from the user's bank account. The user's equipment then unblinds the note and uses it to pay for goods or services, leaving the merchant to check that the signature is authentic and forward it on to the bank, who also checks the signature and credits the merchant for the agreed amount.

The flow of data and goods is identical to that modelled earlier in Chapter 3.

10.2.2 A Sample Ecash Transaction

1. A sum of money is withdrawn from a users Bank to the Ecash Mint.
2. A further amount of money is transferred from the Mint to the Wallet on the hard disk.
3. The coins are automatically given a mixture of values to equal the total of the withdrawal.
4. A DigiCash merchant is visited. The user wants to buy a product and the price is agreed.
5. The merchant's software replies with a payment request, automatically opening the users Ecash wallet.
6. The user agrees with the payment request from the merchant and clicks on 'YES' - thus accepting the funds being debited from the Wallet.
7. The Ecash software automatically chooses the coins from the users hard disk, ensuring that the largest coins are used first.
8. The coins are sent to the merchant, whose software automatically forwards the coins to the bank for verification.
9. The bank replies to the merchant with an acceptance and verification of the users coins.
10. The goods and a receipt are then shipped to the user.

First of all, Ecash *must* be available on a users hard drive before any goods or services are purchased. Ecash can be withdrawn by clicking on the Mint icon in the Ecash status window shown below. The user then simply types in the amount that they wish to withdraw from the account and clicks on 'OK'. This initiates a transfer of funds from the Mint to the hard drive.



An Explanation of the Icons:
Icon 1: Mint Icon - To withdraw and deposit Ecash
Icon 2: Payment Icon - To make or request payment
Icon 3: Notelog Icon - To see the log of transactions
Icon 4: Status Icon - To look at bank account status
Icon 5: Set-up Icon - To change Ecash settings
Icon 6: Coin Status - To check the amnt of coins available

Figure 22: Ecash Status Window and Explanation

At this point, there are two ways with which a user can spend the money. One way is for the user to respond to a request for payment, the second is to initiate a transaction personally.

Firstly, a merchant's software is able to generate and send a request for payment if the user has asked to buy a product or service. This will generate a request that will simply ask the user whether they want to make the payment or not. An advantage of DigiCash is its ability to be configured to automatically respond to future similar requests. A button marked 'Policy' allows the user to set and customise which payments can be made automatically. This is an attractive feature with which to pay amounts to Web sites that are used a lot, such as a news feed.

To make a payment, the user simply fills in the details of the payee. This can be seen in Figure 23.

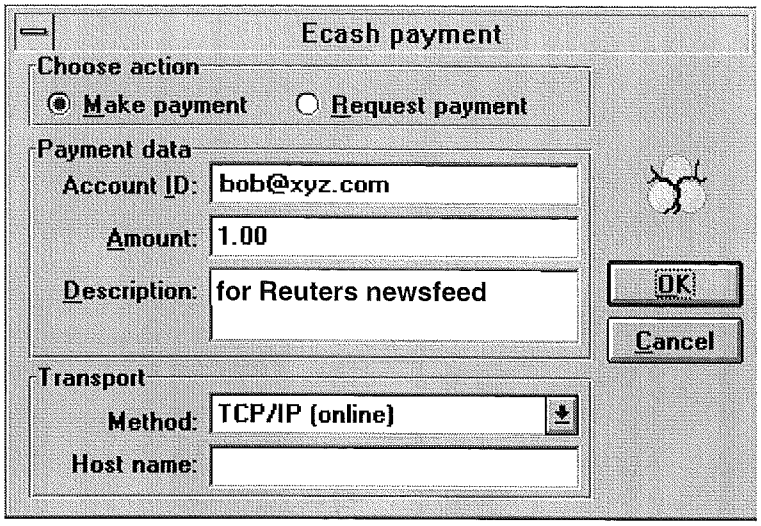


Figure 23: The Ecash payment Window

Receiving Ecash is also very user-friendly. The user has two choices, of which the first is to credit the coins to the Ecash account and the other is to add the coins to the Wallet for future use. The 'Policy' can again be set to automate the process of receiving payments.

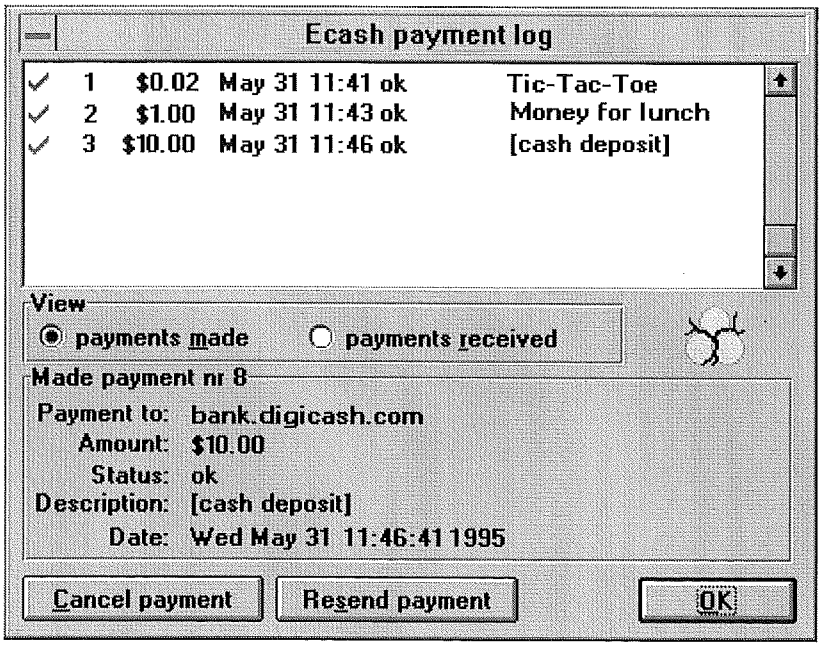


Figure 24: The Ecash Payment Log

As can be seen from Figure 24, the user has an easy and user-friendly way of tracking and checking all deposits and withdrawals to the account. This is available by clicking on Icon 3 of Figure 22. The fields are relatively self-explanatory except for the 'ok' column. The 'ok' signifies that the merchant has deposited the payment, and that the payment is not able to be cancelled. If 'ok' is not displayed, the payment can be cancelled making it null and void. This would present an ideal solution to trying a product before it is bought, but it appears to have no other use. The merits of 'try before you buy' are discussed in the First Virtual payment mechanism summary in Chapter 6.

10.3 SECURITY ASPECTS

RSA cryptography forms the backbone of DigiCash security.

When executed for the first time, the Ecash software automatically generates a pair of 768-bit RSA encryption keys which are unique to each user. One key is kept secret by the user whilst the public key is used by DigiCash to check authenticity. A user that wants to authenticate a message can encrypt it with their secret key, meaning that anyone can verify the message by decoding it with the their public key. A party that wants to send a confidential message encrypts the message with the public key of the receiver. The receiver is the only one who will be able to decode the message.

Due to the fact that the issuing bank has a public key and the user knows the blinding factor it is possible and simple for the user to verify that a payment was made. The user also benefits because when notes are sent to the bank to be signed they are blinded, making it impossible for the bank to align a signing with a payment. It is impossible to counterfeit the bank's signature. In my view this ensures three security conscious benefits of DigiCash:

- The bank is protected against forgery.
- The merchant is protected against the refusal to honour a payment.
- The user is protected against an invasion of privacy.

Another issue is that of double spending a note. DigiCash counter this problem by having the merchant software issue a challenge to the users terminal to respond with some information about the note number. The information discloses nothing about the user, ensuring that privacy is not an issue. If the user attempts to spend the note a second time then the note gives away the identity of the user when the note is deposited.

10.4 EVALUATION

This section evaluates the DigiCash payment system against the features discussed in Chapter 6.

DigiCash is a user-friendly, widely available payment system that creates a novel way to make Internet payments. There is a growing list of banking corporations that are willing to use the technology and this shows that the system has been evaluated well and has true potential.

Security Requirements:
Trustworthiness : Safety : Anonymity

DigiCash is undoubtedly unsafe. The fact that cash is stored on a users hard drive implies that anyone can use it who has access to that particular computer. Its trustworthiness is also compromised with regard to the possibility of a hard disk drive crashing. Although this is not a problem that DigiCash can help with, the implementation of the mechanism implies that this system cannot be fully trusted.

In the case of a hard disk failure, the user is able to retrieve 'crashed' coins but only with the help of DigiCash, or a back up of the hard disk itself. In this way the system is safe. It is also safe as a direct result of a 768-bit key that protects the users' funds that are transferred back to the Mint.

Anonymity is perhaps the strongest feature of the entire system. The system is wholly anonymous but allows users to show their name and addresses if they are needed. This is in direct contrast to the other two systems which do not allow anonymity to be turned on and off. There is only one major concern and this is reflected in the point above. If the safety of the system is called into question and the hard disk crashes, the only way to get the money returned is to ask DigiCash. This means that a user's anonymity must be surrendered so that the key can be used to check the currency.

Commercial Requirements:
Ease of Use : Flexibility : Universality : Expirability : Cost Effectiveness : Reusability

After testing the DigiCash system, evidently some thought has been put into the design of the user interface. The only problem affecting the ease of use is that the user must remember to 'bank' the coins in the Mint when all transactions are completed or a situation such as hard disk failure could arise. This is not enough to detract from the general easy-to-use feel that is evident in both the text-based Unix systems and the GUI-based Windows formats.

Flexibility, or the ability to make a payment without a third party, is not a feature of this system. Payment can be made without passing through the Mint, but can never be cashed without that third party. The fact that payments must be verified on-line also implies that universality is not a requirement that DigiCash satisfies. DigiCash, unlike Mondex, is only available on the Internet and cannot be used over alternate networks.

DigiCash tokens expire, although the ability to exchange expired tokens for unexpired ones is available. This is a key benefit of the system as it allows the company to know how much liability is held by users as tokens. A disadvantage of this may be that the serial number for tokens may become too large. The cost in terms of storing a random token number may be quite high in relation to the size of the rest of a packet. The fact that tokens expire, both by date and by being banked detracts from the commercial requirements by implying that tokens can not be reused.

Finally, as costs are always associated with central transaction processing, DigiCash can not be totally cost-effective. This does not appear to detract from its ability to handle micro-payments.

Constraints:
Acceptability : Integration : Non-exclusivity

DigiCash is perhaps the most extensively acceptable mechanism, that has a strong software system which integrates well from a user's point of view. For most users the concept of tokens may be new, but the use of tokens in certain situations suggest that their use is not a major obstacle. It's acceptability as a payment mechanism does not therefore need to be questioned. However, integration provides more of a problem. As stated, the user software integrates well with other software on the desktop but from a merchant's perspective it appears that the system does not provide features that could be expected from other merchant software. The system does not provide any functionality enabling it to integrate with, for instance, database programs.

10.5 SUMMARY

DigiCash is a strong system concerning storing and monitoring spending of e-cash. However, it does have some disadvantages:

There is no technique behind recovering e-cash from a corrupt hard disk without losing anonymity. By making the same key, it is possible for a user to get all the withdrawals back and then re-deposit them (which the client software does automatically). There appears to be a user option at this point: having all transactions revealed, losing anonymity and getting the cash back or losing all the cash and staying anonymous.

The problem of having a corrupt disk implies that most users will make frequent back-ups. Therefore, the risk is run of restoring from a failure and having e-cash available that has already been spent. The problem appears to be that as e-cash is cleared on-line, e-cash that has previously been spent will generate errors, others will be deposited. There is no idea of 'fraud' within the on-line clearing system and there is no way to tell whether a coin has been spent, short of trying to deposit it.

This situation also shows that there is no way to tell how much an off-line payment is worth without actually loading it into the DigiCash system. Of course, it is possible to be told how much a given

payment is for, but if it is not cleared with the banks there is a chance that whoever made the payment will cancel it before the money is received.

An advantage of this system is the ability to make off-line e-cash payments. By selecting the `METHOD = off-line` a text file would be created with the e-cash payment. By putting that text into an e-mail it is possible for the payee to read the payment directly into a Mint account.

DigiCash's other main advantage is the security of the system. It is not possible for the bank to have list of the serial numbers of the coins that are produced because it never knows this information. Each coin is created by a user's client software, which chooses the serial number at random. When it is sent to the bank to be signed, blind digital signatures are used so the bank never sees a coin's serial number until it is deposited.

Although each coin can only be used once, there is a probability that at some stage the system must run out of coin numbers and eventually recycle some numbers. With each transaction, an existing coin is destroyed and a new coin is minted (a transaction does not always have to be a purchase). This problem may be solved by making the numbers very large, maybe in the order of twelve to fourteen bytes per serial number.

CHAPTER ELEVEN

PUTTING THE SYSTEMS INTO PRACTICE

11.1 INTRODUCTION

After discussing the three systems in-depth, it is important to evaluate them against each other to enable us to see where each strengths lie and in particular, which one will make the perfect on-line electronic commerce payments system. Before pitting the features of the mechanisms against each other, this chapter looks at three potential scenarios that a payment mechanism could face, and examines how each method of payment would suit the situation. The situations are completely hypothetical and are not of any direct consequence of the research of this report. The situations are designed to ensure that a broad spectrum of characteristics are tested.

11.2 THE HYPOTHETICAL SITUATIONS

By giving three potential scenarios to test each system it should become evident how each system responds to the needs that are required from them. As mentioned previously, the situations are designed to test each systems particular strengths and weaknesses.

11.2.1 Situation One - Anonymous Data

Situation One examines the need to send a Valentines Day e-mail card over the Internet. By assuming that all Valentines cards are sent unsigned, it is assumed that the sender of the e-mail will want to remain anonymous. Therefore the mechanism used for payment should leave no trail as to who sent the card in the first place. It is also assumed that as the card is no more than a small file being transferred across the network, then the cost will be minimal. Therefore a payment system that can satisfy the request should be able to handle micro-payments in a quick easy and cost-effective manner. For ease of use and by assuming that many millions of Internet users will want to send a card, the payment system should also be one that is widely acceptable and accessible, potentially being able to be used by anyone, anywhere.

The features that this situation require are thus:

- Anonymity
- The ability to handle micro-payments
- Universal acceptance
- Cost-effectiveness

In this situation, the credit based system would be discarded immediately, due to its inability to handle micro-payments cost-effectively. Therefore, a decision has to be made between the token system and the cash-based system. Both are cost-effective but unlike a credit-card system they do not generally have universal acceptance. It is also evident that both are strong when it comes to handling micro-payments.

Mondex is not wholly anonymous. When a transaction takes place, the identification of the card with which a transaction is taking place is shown on the LCD screen (if the transaction is completed with a wallet). There are also transaction numbers that could reveal whom a payment was made with. This information is not generally available to the public, but it does imply that a transaction is never truly anonymous.

In contrast a transaction with DigiCash would be blinded by the user and signed by the bank. This ensures that the user is protected against an invasion of privacy as the bank cannot align the signing of a token with its payment. This is one of the unique features of DigiCash. When paying with e-cash the identity of the payer is not revealed automatically. The negative features of DigiCash are that there will

be a cost levied on the transaction to take into account that it is centrally accounted and that to utilise the system a bank account must be opened with a DigiCash supplier - of which they are presently none in the United Kingdom.

Evidently DigiCash is the best method for payment in this situation, although the price of having anonymity is that transaction fees must be paid. The problem of having zero issuing banks in this country is countered by the ability to open a Sterling-denominated account at most DigiCash banks. Mondex would also be acceptable in this situation, as a merchant would be more willing to accept immediate payment than having to change a token. The lack of anonymity is an allegation and the probability of someone finding out the details is still relatively small and does not outweigh the advantage of being able to make micro-payments easily. However, Mondex is not yet operating on a global basis.

11.2.2 Situation Two - Physical goods

In contrast to the first situation that involved buying a 'virtual' product, e.g. data, this example looks at buying a physical product. In this case, the product is a brand new Ford Escort, bought direct from Ford's World Wide Web pages. Both the buyer and the seller in this example have requirements that the payment system must satisfy. The most obvious is that it must provide the ability to make macro-payments and include a very secure payments' infrastructure.

The buyer would have two serious issues. The first would be that he could prove that he had paid the money to the company, implying that a payment system should be traceable (and not anonymous). Secondly, it is assumed that the buyer would not want to pay for the goods before they were actually received, thereby suggesting that delayed-payment would be a beneficial feature.

In contrast, the seller would want proof that payment is available before they deliver their car to the buyers address. They would also perhaps like to integrate their payment system with their customer databases so that they could build a customer profile. There are many other 'wishes'. Ford may prefer that the payment was not anonymous so that there is an ability to register the car with the authorities or buy a tax disc in advance.

With this example, there may even be a requirement to pay for the car in a currency that is not the national currency of the country. The payment system may therefore be required to support multi-currency transactions.

The features that this system requires are therefore:

- Traceability
- The ability to make macro-payments
- Multi-currency transactions
- Integration with other software

The three systems evidently provide characteristics that differ. Although it has been shown that DigiCash is the preferred method for making low-value anonymous transactions, it is possible for a DigiCash user to identify himself but only if he chooses to do so. It is assumed that functionality built into Mondex software will also allow a user to identify themselves if they so choose, although this by no means guaranteed.

It has been stated that a function of Mondex's security is that cards are assigned a maximum value that can be held on any given card, and that most people will be assigned limits that run into hundreds of Pounds rather than thousands. This limits the value that can be spent in any given transaction. By making the assumption that a user can gain special exemption from low card limits or by assuming that the card used to make the purchase is a company card (with a much higher limit) then all three payment mechanisms can be recognised as being a valid form of purchase for this type of payment.

CyberCash is not anonymous due to the transaction logging that takes place, yet this does not detract from the benefits of using it as a payment system in this situation. The ability to charge the purchase to a credit card ensures that that the product is insured for delivery. The fact that it is a credit card payment also implies it is more likely to be acceptable by the merchant. At present CyberCash do not offer global currency transactions, which therefore means that it is not suitable for this situation. CyberCash currently offers purchases made only with US dollars and only at on-line merchants who have a US bank account. Eventually, they will be able to be used outside the US with any foreign or International bank that is a CyberCash issuing bank. When a consumer buys a product or service on the Internet listed in a foreign currency, the system will automatically translate the currency and the debit will occur in the consumer's domestic currency. Where CyberCash fails, Mondex shines as it can successfully handle multi-currency payments in a user-friendly way. By questioning its anonymity as in the previous section, it may also be traceable.

The problem is therefore to differentiate between DigiCash and Mondex for making large payments. Mondex is probably the best way to make macro-payments as it provides guarantees that a transaction is completed, can handle multiple currencies and is not reliant on being attached to one particular network such as the Internet. By providing a log of past transactions both parties can confirm that a transaction has been successfully completed. Its downfall in this area is the inability (at the moment) to be able to interact with other software or provide any major details of the user if they were required. The major obstacle against DigiCash is its inability to handle the currencies. For this reason, it is arguably DigiCash that is the best payment system for this scenario, as the integration of its software with other software is a key advantage. When CyberCash becomes a true global system, there is no doubt that this would be the preferred choice as it offers product guarantees, world-wide acceptance of credit cards and full software integration.

11.2.3 Situation Three - No Data or Goods

The third scenario is that of an on-line lottery. The main feature of an on-line lottery is that it could be a mecca for Internet payments. By implication it would be a haven for hackers as well. A payment system that wishes to use an on-line lottery should therefore be secure, with strong cryptography protecting the players. From the opposing side, if a winning payment was made, a user will want potentially want to remain anonymous and the payment mechanism must provide for this.

The ability to play the lottery by using off-line payments and the ability to make regular payments may also be requirements for a lottery player.

Key features of this scenario are:

- Secure transactions
- Micro-payments
- Anonymity
- Off-line capability
- Configuration of payment regularity

The first assumption in this scenario is that payments are going to be small and frequent, rather than large and infrequent. For this reason, the selected payment mechanism must be extremely cost-effective or the lottery operator will have to charge a fee to cover transaction costs. This is the case for Interlotto [INT], a legal Internet lottery scheme that accepts credit card payments. Secondly, it is necessary to have a fast-payments approach in case a user wants to make a payment just before a draw takes place. It is noted that there may be a trade off with regard to secure transactions and fast payments. It is the author's opinion that in this situation speed of transaction is not as important as the security of payment details. It is also noted that speed is affected by network bandwidth and many other variable factors so that the speed of encrypting a payment may form only part of the delay of actually transmitting a payment.

Mondex would be able to handle this situation well as it is ideally suited to micro-payments. An account is only debited when the transaction is complete meaning that a user would know whether a last minute entry to the lottery had been accepted or not. This is a benefit that the alternative systems can not emanate. On the negative side, Mondex may not be wholly anonymous and without the software it is not possible to know whether software will be able to schedule regular payments from a hard-disk based wallet.

One major benefit of DigiCash is the ability to make off-line payments, meaning that payments could be sent by e-mail or rather than through the DigiCash system. To a lottery player, this would be a good way around a potential situation where the network is not reachable, and is a feature that is not offered by the remaining two contenders.

CyberCash immediately fails to suit this scenario due to the high cost of bandwidth when it encrypts as it utilises RSA on a 56-bit DES key. CyberCash is not effective for low-cost transactions either and this is reflected in the SFr2 charge that is levied for Interlotto credit card entries. The overhead costs of having an intermediary also fare negatively against DigiCash. However, DigiCash payments can be anonymous, and the software can be easily configured to make payments on a regular basis for any amount. These are two functions which Mondex is currently incapable of, and it is for this reason that DigiCash is probably the best payment method in this situation, although it is not perfect.

11.3 ANALYSIS OF RESULTS

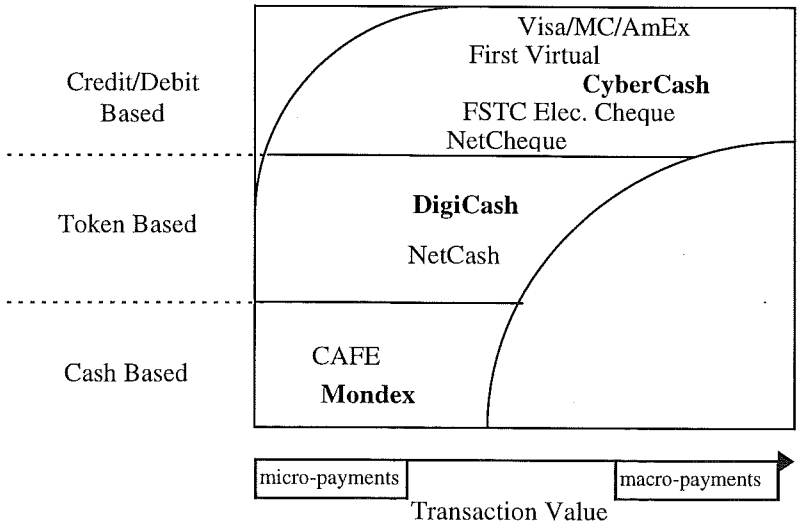


Figure 25: The Analysis of On-line Payment Systems

The above diagram depicts the findings of this project, considering a mixture of what has been delivered and what is due from the companies involved. It can be seen that DigiCash is placed in the middle of the diagram, implying that it is best suited for medium sums of money but still usable for larger or small amounts. The diagram also proposes that CyberCash should be the preferred method for macro-payments but is still usable for some micro-payments. Vendors such as IBM are working on solutions to accrue credit card transactions until economic-sized balances are reached.

The results to this project are quite surprising, with DigiCash beating Mondex and CyberCash in all three hypothetical situations. The implication is therefore that DigiCash is far and away the most useful system, and from this it will be the system that most people choose to use. However, it is not wholly possible to say that one mechanism is best. It is evident that DigiCash has more problems to be solved and that Mondex will not be a favoured method until it releases some software. It must also be noted that although CyberCash did not do particularly well in the hypothetical scenarios, this is due to the fact

Secondly, given any account ID it is possible to determine an account number by guessing that at the early stage of system implementation that most account numbers will be only 4 digits long (and preceded by 6 leading zeros). The cost of a correct guess is a payment of $0.01, which can be cancelled in due course. By generating a payment of $0.01 to anyone@anyhost.com and trying to deposit it into each 4-digit account number, it can be seen that only one account will accept the payment and not return an error message. This is therefore the account number that ties in to the account ID. After the payment is generated and accepted it is possible to cancel the payment. When this is done, if the user tries to deposit the same (cancelled) coin into each account number, most accounts will return 'wrong userID', but one will return 'coin already spent'. Thus, it is possible to determine any user's account number, and thus the balance related to it.

The second fault lies in the ability to use a packet sniffer to watch the unencrypted 'Deposit' messages that carry information correlating account numbers to account ID's. Although both of these methods are not an efficient usage of time, they successfully prove that personal information is not secure. The work factor to determine the account number is proportional to the size of the space of the account numbers. Currently this is not very large as the amount of users is small. The implication is that DigiCash is not fully secure.

A third problem appears to be that by using a packet sniffer it becomes possible for someone to maliciously 'use' someone else's money. The owner of the coin can potentially lose the use of a given coin whereas the hacker neither gains or loses from the situation. This is done by 'stealing' the list of payments and deposits of on-line coins. The following code shows the description of an on-line coin, where the encryption of the signature is carried out by the equation (f(n)^(1/n) XOR f(payment-hdr)) [DIG].

```
onl_coin=
[
int keyversion;
MPI n; coin number
MPI sig; encrypt coin signature
]
```

It is evident that the coin number is at no stage encrypted leading to the problem that if the message is seen by User A, A can use the same value of n to withdraw a coin from the account BEFORE that coin is spent by the original owner. User A does not need to spend the coin, it can just be withdrawn and then re-banked. In this way, the original owner loses the use of the coin and User A does not gain or lose. To ensure full security of the system, it may therefore be necessary to change `onl_coin` to include the encryption of n, as illustrated n the following code.

```
onl_coin
[
int keyversion;
(MPI n; coin number
MPI sig; encrypt coin signature)
]
```

This should make the possibility of causing damage less easy.

It can thus be seen that while encryption algorithms ensure the safety of some details, they do not ensure the security of the entire mechanism, just certain parts.

11.4.2 Exchange Agreements

Another important issue that emerges is whether exchange agreements will be imposed on e-cash issuers. In a true electronic society, one e-cash user should be able to use their cash on another person's system. EUNet of Finland and Deutsche Bank of Germany are both currently issuers of DigiCash's e-cash.

The question is therefore:
If User A signs up with EUNet and Merchant B signs up with Deutsche Bank, can User A buy from Merchant B?

In theory EUNet and Deutsche Bank would need to have an interbank clearing agreement. If User A sends e-cash to B, B would have to contact Deutsche Bank. As DB recognises EUNet's money, it would contact EUNet and clear the currency. EUNet could then credit DB's account held at EUNet. Following this, DB could acknowledge this to Merchant B, who could then ship the goods to User A

However, this assumes that the reason DB contacts EUNet is to confirm that the e-cash has not been double spent. Once this is confirmed, the two banks do not need to contact each other. EUNet does not have to credit Merchant B's account as there is no transaction between DB and User A. The transaction is between Merchant B and his bank, Deutsche Bank. In theory, the moment that EUNet confirms that the e-cash is valid, then DB already owns it.

The second assumption is that e-cash is truly an open standard, which is to say that it is a widely acceptable means of payment. This implies that any e-cash bank is obligated to accept e-cash deposits with one condition: that the issuing bank must validate it. This could be compared to the current cheque clearing system.

The third assumption is that e-cash users have faith in the issuing banks. As insurance does not apply to e-cash, it is true that savings in e-cash will not be applicable for the deposit protection scheme in the United Kingdom. It must be said that ultimately very few e-cash issuing banks will fail, as they are generally backed by 'real' banks, but we must note that it is possible.

The major problem is if the banks do not agree to exchange cash It is perfectly plausible that an issuer would not accept e-cash as it had not issued it in the first place. This would put the universality of e-cash into some jeopardy. If an issuer chose not to accept certain e-cash, it would not lead to the collapse of a system, or make e-cash useless. It would only put conditions and boundaries on its use.

The situation above means that there is a difference between the acceptance of e-cash and the validation. One may take place without the other. The validation of the cash means that the receiving bank checks with the original issuer to see if the tokens have been double spent. The acceptance is the acceptance of e-cash as a deposit.

If EUNet refused to validate any non-EUNet e-cash, this (as stated above) would not necessarily lead to the complete failure of the system. It does mean that EUNet's customers would not be able to accept payments from non-EUNet customers. This can be seen to be a huge constraint on trade. To proceed from this situation it would be necessary for each customer and merchant to have multiple e-cash accounts with multiple issuers. This means that there is potential for hundreds of issuers and a very competitive marketplace.

A different solution may entail EUNet's customers actually bypassing EUNet and validating received currency direct with the issuer. This would allow EUNet's customers know that an accepted deposit is valid and has not been double spent. A drawback of this is that EUNet may still not accept the cash as a deposit.

With this said, it would appear that there are two 'wants':

- Independent verification of e-cash.
  This would allow merchants to check that e-cash has not been double spent.

- Interbank acceptance of e-cash.
  Any issuing bank should accept any other banks' tokens.

Independent verification of e-cash: On the basis that there will be millions of e-cash transactions, it is true that the amount of time that banks would spend verifying tokens would be high. Therefore it is necessary to find a way to allow verification to take place more effectively and efficiently. A solution to

that its coverage is purely United States-based and as the situation changes the ability to make multi-currency payments and the ability to have more advanced features within the software will convince users that it is a worthwhile system.

One approach to the results is that DigiCash is more complete than the other two systems and because of this it suits the hypothetical situations better. Its functionality is many times greater than Mondex's, but the Mondex card is already being used for telephone transfers in many pilot projects across the globe. DigiCash's functionality is also far better than CyberCash's, yet CyberCash transactions are only limited to the continental United States at present. What does this prove?

Mondex is bound to be a global contender. The amount of banks backing the payment method underlines how powerful the system is. It is a true representative of cash, is decimal based and allows for peer-to-peer transactions. The limit of only five currencies may prove to be inhibitive, but as chips become smaller and more powerful the system may prove to get better. Its poor performance in the situations was almost entirely because of the lack of Internet software. When this is developed, its suitability for situations such as the lottery, or purchasing a car will become more apparent. It is surely true that most retailers, no matter what they sell will want to receive 'real' cash as opposed to a token with which they must validate. Mondex is also the most user-friendly system and has the advantage of being able to conduct transactions over the telephone network as well as over the Internet. The cost of card readers will no doubt drop as their usage becomes widespread.

CyberCash was a disappointment within these tests. Although it is only an open extension of a closed system, its inability to function was highlighted by these tests. CyberCash provides an efficient and secure route of making credit card transactions. The problem with the system is not only the fee charged as a percentage of each transaction, but the strong security that slows the system down. It can be seen that the strong security is ideal in a macro-payment situation, but not so good for other payment amounts. The software is easily integrated with other point-of-sale systems and is therefore extremely efficient for a merchant to use. The main reason for failure is evidently the fact that it provides no extra functionality above the standard credit card transaction. However, people will always be ready to use a system that has a recognisable feature and in this case it happens to be the Visa and MasterCard trademarks. The potential for this system is great, as long as costs become bearable and computing power becomes cheaper.

DigiCash provides a very positive picture with the results of the three hypothetical situations and this is due to the fact that the software is virtually complete. It handled the difficult conditions well in every situation, which was a surprise and each scenario was clinched with a different 'feature' of the mechanism. The software appears to be very powerful, but looks can be deceiving and this system does not feel natural to use. Transferring money in and out of a bank account to ensure that it is insured does not fare well against the other two systems. This mechanism is the most different from current physical cash solutions.

11.4 ANALYSIS OF PROBLEMS

11.4.1 Security

The merits of each system are similar, with the key feature of each system being security. The three approach safety in a different way: Mondex uses its 4-digit PIN as a key security feature, whereas DigiCash highlights it 768-bit encryption technology. However, as discovered in the individual chapters, security is perhaps not as good as the companies' on-line brochures would suggest. An example of this are the suggestions that Mondex may not be infallible [COR], and the two bugs that are present in the DigiCash system.

The first DigiCash bug is relatively simple. By assuming that a 10-digit account number is known it is subsequently easy to determine the account balance, even if it is not owned by the user. This is achieved by sending a deposit of 0 (zero) coins to the account that the bank will accept a deposit. On acceptance, the bank will automatically return an acknowledgement and the account balance.

this could be based on DNS (Domain Name System). If each e-cash coin had information pertaining to the name of the issuer, a user could 'ping' the original issuer and receive a reply with information to whether or not the coin was valid.

Interbank acceptance of e-cash: On the basis that the Bank of England prints the nation's banknotes and the other banks always accept them, it is important that whoever issues the e-cash ensures that its competitors realise the value of its money.

It is evident that the only way that DB could verify with EUNet that the cash it has received from Merchant B has not been spent is by actually sending it to EUNet. Therefore there has to be a transfer from DB to EUNet and then can EUNet credit DB's account. Making transactions in this way means that net settlement is possible.

By introducing clearing centres to the problem, the implications are that they would potentially cause bottlenecks and network congestion. In addition to this, merchants could be expected to want access to clearing centres. The benefits are measurable: Firstly, as the system is decentralised there would be no demand on a bank to certify e-cash, and they could bring costs down and spend more time on improving their systems. Secondly there would be less fluctuation in bank's cash holdings, meaning that less time would need to be spent ensuring that their government-set liquidity ratio's are legitimate.

11.4.3 Usage of E-cash

Widespread use is also encouraged by making the system available to as many users as possible. Mondex has not released any software yet, but their smart-cards are widely available to make telephone-network transactions. The DigiCash and CyberCash software is available in a variety of formats:

IBM - PC

Microsoft Windows 16-bit	Microsoft Windows 95	Microsoft Windows NT

Apple - PC

Apple Macintosh System 7	Apple Mac Sys 7 PowerMac

Unix

Linux	FreeBSD	A/UX
HP-UX	SGI	NeXTstep
BSDI	OSF/1 (DEC Alpha)	SCO Unix
Solaris 2.4 for Intel	SunOS, Solaris or NetBSD	

The list appears to contain the great majority of operating systems available. Unfortunately it does not take into account the fact that there is still a great user base for people with old 16-bit computers such as the Atari ST and Commodore Amiga, as well as a greater number of people using personal organisers and Personal Digital Assistants from Psion, Apple and Casio. The advent of mobile phones with built in 'Organiser' functions such as the Nokia 9000 [NOK] imply that remote banking cannot be that far away. The software companies do not appear to realise that the first people to use these phones are probably the first people who will use Internet commerce technology and the software in these formats is therefore desirable.

To counter this, I believe there are two solutions. The first would be to make a simple ANSI C version of the client software available which would not feature a graphical user interface. This would make the software slightly more portable, although arguably not for handheld machines. A second recommendation would be to make the source code free or shareware, so that unsupported platforms can have GUI's implemented for them by their users. This would help establish a bigger base for electronic cash usage.

11.4.4 The Potential for Fraud and Real Risks

An important issue is whether the potential for secure global commerce is outweighed by the potential for fraud. One assumption is that given any payments system, there will always be people trying to break into it. There is no barrier to stop someone advertising a lottery selling a 'ticket' for e$5 and simply returning a 'sorry, you lose' message. None of the customers will be happy and the owner has the potential of enormous profit. In response there will obviously be extremely bad word of mouth on many newsgroups and currency issuers 'blacklists' but even if the word spreads around the globe quickly, there is no way in which it can reach every single potential customer.

This is a possible situation and deserves real thought. Since e-cash is uni-directionally untraceable it is not possible for a crooked merchant to cheat someone and accept e-cash. This is because the cheated customer can mathematically prove that the money was paid. So, if a transaction has a contract that both parties agree to and digitally sign before exchanging the goods then the cheated party can sue the other for breach of contract.

There are potentially more important risks than this. Internet commerce has to be made as safe as possible so it is imperative to assess the risks to any given system. These may be:

- The situation when the worst case scenario happens
- The frequency of abuse to the system
- The failure of service that occurs due to a crisis

Using the credit/debit model as an example, it is probable that the worst case scenario would be one of which a thief broke into the system, located the database records of credit and debit card numbers and then maliciously used them. For the cash-based model, the equivalent may be that someone successfully manages to tamper with the tamper-proof smart card. In any case where credit and debit card numbers are transmitted over a public network and stored, encoded or decoded on a computer, the risk of a break-in is relatively high and the merchant can be seen to be a target.

The major problem with payment schemes that simply encode data and then send it over the Internet is that there is a single 'bottleneck' failure point. If a criminal managed to find a single bug in the encryption algorithm or releases a virus that steals code as it is typed into a 'secure' browser, it is highly possible that numerous credit card numbers could be collected.

It is true that sophisticated cryptographic systems such as RSA and DES reduce the vulnerability by moving the decryption to the charge-aquirer's Internet-connected machine which in effect reduces the amount of machines for criminals to target. Its adverse reaction is that each criminal will spend more time targeting the fewer machines that are available. In the case where there are fewer machines, each bank or issuer implicitly needs a high level of Internet security knowledge to ensure that safety of the transactions is one of its priorities and that the level of security is in direct relation to its level of liability. At the moment, the author does not believe that this is happening.

The 'frequency of abuse to the system' assessment is an issue that can only be assessed over time and exposure to the Internet. It is not possible to second guess the amount of break-ins that can occur, and it is known that some companies cover them up if they do occur [CIT]. During the course of this project it has also become evident that most of the cryptographic functions are only computationally impossible at the moment. No doubt computing power will catch up, implying that at some stage cryptographic solutions can experience worst-case failures with potentially catastrophic consequences. It is not inconceivable that this could cause the collapse of the entire credit card based system.

One way of making the system as safe as possible would be to create daily or hourly multiple back-ups and ensure that the system has a great deal of redundancy. This is analogous to the situation of a power station, where a system may have a single component that can possibly cause a catastrophe if it fails. To counter this, redundancy ensures that a failure will almost certainly activate a back-up procedure, that is possibly coded to the same specification but in a different way.

According to Neumann, an alternative and complimentary way to ensure that system safety is kept safe is to set up multiple barriers in the way of a would-be thief. These could take the form of multi-layered firewalls, meaning that an intruder getting through one firewall would still have to get past the next one. It also possible to set feedback alarms at each level of firewall to report that an intrusion has taken place [NEU].Of course, each firewall would have to be separately coded.

At this point it is important to note that generally cryptosystems do not have or provide redundancy or the back-up systems that are needed. An alternate rule could be to keep the system simple and user-friendly for the merchants and users. It is easy for people to use systems and interfaces that they are familiar with. However, they are not likely to learn rules to ensure the safety of transmission. It is for this reason that simple rules are given by credit card companies... 'At a restaurant, do not let your credit card out of sight'.

11.5 CONCLUSIONS

It is apparent that DigiCash fared well throughout the test situations and proved that it is reliable and useful system. Its use is generally suited to all payment situations but only while the other payment systems are lagging behind in terms of implementing a global payments service. The list of banks franchising a DigiCash system is growing which will lead to a surge in acceptability of the system. Until problems such as any user being able to find an account balance are corrected, users will be hesitant on using the system for anything major, perhaps just to download a data file every so often.

Mondex, although sparse of functionality may prove to be a surprise. As it is usable off-line to make payments in shops as well as peer-to-peer transactions, it has very high potential. The ability to make immediate cash payments implies that merchants will be very willing to implement the system. It fared well in the tests but until true on-line purchases are available, it is hard to measure how the card will perform. The use of smart-card readers is a barrier to entry for this system that may not be overcome easily.

CyberCash did not perform well in the tests. Its inability was defined by its preferred payment method and by the boundaries to use that currently exist. The software is strong and it is a sound product that delivers exactly what Internet merchants require. The ability to integrate the system with other card reading interfaces is a benefit which Mondex will eventually try and emulate. Although the usage of credit cards imply that the system does not move forward the barriers of electronic commerce, this may be its biggest selling point. It certainly enables a familiar payment method to be securely used over an insecure channel and it does not require any pre-registration to use. A user can simply download the software, type in the credit card number and then buy a product. For this reason alone, CyberCash may be many users first foray into on-line commerce.

No system is 'best'. They all have different solutions to different problems and can potentially co-exist. Although DigiCash triumphed in the hypothetical scenarios it is evident that Mondex could eventually be better suited to making immediate micro-payments whilst CyberCash would be better suited to macro-payments. DigiCash's role would then be relegated to being suitable for making regular micro-payments, such as for data.

The author believes that credit cards will sustain their lead despite the proliferation of payment systems. Credit cards mechanisms should benefit from more advanced security, regulatory protection, and consumer familiarity. The digital cash solutions will lag behind for macro-payments but will definitely find a niche in micro-payments. There are three prime reasons for this:

- Credit Cards can still enhance security.
  The secure electronic transaction (SET) standard created by Visa, MasterCard, Netscape, IBM and Microsoft will enable consumers to receive digital certificates to sign encrypted credit card numbers for authentication. Merchants cannot decrypt the numbers and the system protects users from fraudulent merchants and shields merchants from stolen credit cards.

- Credit cards require no change in users behaviour.
  People already order goods over the phone with their credit cards. Credit cards are able to be used without the need for cards to be presented. Also, many users use credit cards because of additional benefits such as Air Miles or special rebates.

- Micro-payments can be supported.
  Micro-payments can be combined and charged in total to a credit card. The charges can be accumulated until a set value is reached or for a specific time period.

It may also be noted that the complexity of the token and card systems and their unfamiliarity towards consumers may give credit models a boost. Digital cash really requires too much technology overhead to protect against fraud and counterfeiting. It suffers in three key areas:

Firstly, it is inconsistent with human behaviour. In the United States, the largest Internet market, consumers do not use multiple currencies. Buying Web currency will be like buying foreign currency, but why should people do this in their own country? Furthermore, it is possible that competing currencies and exchange rates will confuse consumers and frustrate merchants.

Secondly, the currencies are currently issued by unfamiliar companies like NetCash, FSTC and DigiCash. No regulations exist to protect consumers from fraud or loss with a digital currency. If the cash is to reside on a user's Hard Disk, users' must worry about PC theft or Hard Disk crashes.

Thirdly, complexity of the systems will limit the acceptance. All the systems are user-friendly, but hardware solutions do have limited appeal: Consumers do not have the hardware that is needed, distribution methods are unclear and it is uncertain who will pay for the devices.

11.6 SUMMARY

DigiCash is evidently the only complete system available. Three hypothetical situations prove that it provides a sound basis for a payment system and that it is capable of handling the most demanding situations. As representatives of entire payment models, Mondex and DigiCash prove that their models are sound in theory but lack in implementation. The scenarios reflect the lack of functionality that is present in the systems.

The ability of these companies to introduce incomplete payment systems coupled with major inadequacies present a scenario in which electronic cash is not a feasible opportunity for the majority of Internet users. Until issues such as exchange agreements and portability are answered then users are going to be wary of trusting any mechanism that cannot provide guarantees.

It is also argued that there are potentially more harming issues than the problem of fraud. Internet commerce has to be made as safe as possible by assessing the risks to a system in advance of the implementation and being proactive in implementing the solutions. By ensuring that secure browsers are genuinely secure and that gateways are robust it is possible to reduce the vulnerability of a given mechanism.

All three systems can find a niche in the Internet payment systems hierarchy. With each system arguably suited to a particular level of cost-effective payment then the ability to conduct transactions in a user-friendly and easy way is not far off. When the payment companies release full versions of their systems, then and only then will it be possible to deduce which is 'best' and which can serve the Internet community in the best way.

CHAPTER TWELVE

FUTURE TRENDS IN ELECTRONIC COMMERCE

12.1 INTRODUCTION

This chapter provides an insight into the trends that can be expected to be seen emerging in the field of electronic commerce that are concluded from the study of the subject. By assuming that future will build on what is presently in use, the chapter takes an in-depth look at what will be needed to conduct transaction in a secure, efficient and user-friendly manner.

12.2 TRUE ELECTRONIC COMMERCE

There have been a great variety of payment mechanisms proposed for Internet commerce, the majority of which are initiated by technology companies rather than banks or financial institutions. Their aim is the same - to enable existing real-world payments mechanisms to move over to virtual payment systems.

It is true that for companies such as CyberCash which use credit cards as their payment vehicle that they have made the first and most important step towards true electronic commerce. However, the mechanisms proposed do not provide the flexible payment systems that are needed to allow the Internet and the Web to be exploited in a proper manner.

It can be said that cash is effectively stale. After being used for nearly two hundred years, it is evident that it costs a great deal to store, administer, distribute and bank. On top of this it is unsafe and insecure. The ideal mechanism for the Internet therefore is an electronic equivalent of cash, that rids itself of all the negative features of cash but builds on all of the positive functions.

What the author is effectively saying is that cash should be dematerialised. In other words, what is needed is both:

- Credit and debit facilities.
  These would allow guaranteed high value transactions with certified retailers. The costs associated with having a guarantee and the convenience of a later payment would possibly be a transaction fee as well as the loss of anonymity.

- Electronic cash
  These would be anonymous but safe low value transactions with any (non-certified) merchant. The implicit cost of having no guarantee and privacy is that payment is due immediately and there is an increased risk of a merchant not supplying the goods requested.

Digital cash does not have to be designed to faithfully mimic all the properties of physical cash. It can as demonstrated, be implemented to preclude some features of physical notes, such as complete anonymity, while including other attributes that are not possible such as full divisibility, assignment of spending limits and links to the current owner.

Many of the electronic commerce initiatives that have been studied vary in their approach to security and anonymity, their ability to handle micropayments and their applicability to various types of transactions. They also differ in their business models, most notably with pricing strategy, but also as to their assumption as to what markets they are aiming at.

The diversity of payment methods at the level ensures that there is customer choice but more importantly in the sense of this project, it is an enabler of innovation. The continued innovation will enable more features to be added to the systems and will encourage merchants to accept 'alternative' currencies.

At the risk of sounding undecided and after examining numerous payment systems and three in detail, it should be noted that no single system is best. Which system is adopted depends largely on the needs of the transaction. According to survey data, the single most important factor is wide acceptability of the system [SUR].

It may therefore be that any system, whether it is formally standardised and secured or not could gain market dominance and remain in that position by virtue of its ad-hoc standard. Merchants would use it because their customers use it, and vice versa.

The main channel for competition would not be in the price basis of the mechanism but in gaining exclusive right to the point-of-sale systems of a large number of Internet retailers. The advantage of this would be that it makes electronic commerce payments available in a relatively short timespan. Unfortunately this is not conducive to diversity of technological advancement in electronic commerce. In fact, it could be seen that this would be analogous to the tri-opoly of Visa, MasterCard and American Express in the British credit card market.

An alternative to this situation would be the adoption of one standard electronic payments system. In this case, any intermediary would jointly adopt an inter-operable system whereby the client of one system could transparently conduct transactions with any other merchant whose intermediary has jointly used an inter-operable system.

A system such as this would possibly enjoy two advantages over a proprietary payments system. The first of these is choice. Choice would ensure that there is better service. As competition increases the amount of intermediaries vying for business, users would have to differentiate between the services provided. The second benefit is that of simplicity. An open standard would provide consistency in payments from the user's view. The survey shows that simplicity is the second most important aspect that is looked for in an electronic payments system.

However, as there are so many systems available, wide acceptance is not gained as easily and to make a truly global payments system a framework is needed which encompasses the following requirements. These findings are a direct result of the unanswered problems listed in Chapter 11.

- Interoperability
  Electronic commerce must be based on a common set of services and standards that ensure interoperability. The use of RFC's may lead to a standard becoming accepted.

- Maximum Flexibility for Innovation
  This project has mostly looked at the need for micropayments. No-one can second guess the future which may have no need for petty services that require these small payments. Therefore the electronic commerce framework must be flexible enough to address any requirements that arise as well as any changes that occur. If one payment systems encompassed the benefits of having real cash on a card (like Mondex), that could schedule automatic payments (like DigiCash) but utilise the existing financial networks (like CyberCash) then a very flexible payment tool would be created.

- Information Intensive Products
  As above, this project has looked at the requirements of downloading small pieces of data. As technology advances, it is evident that the role of data will become more important. In a management sense products will become enabled by I.T., as opposed to just being distributed by it. Therefore the payment system should be required to allow product designing, billing, payment and details as an integrated process.

- New Usage of On-line Systems
  Electronic commerce will need at some stage to support advanced payment options that are currently not available. These may include payment in advance for products, the e-cash equivalent of direct debit or pay-per-use shareware. This sort of usage is ideally suited to a low cost distributed environment such that the Internet provides.

- Heterogeneity
  There are still many legacy commerce systems existing in this arena. A successful infrastructure must let users transparently transfer funds between older systems such as EDI and newer systems.

A framework developed with this in mind will form a basis for a powerful and useful electronic commerce infrastructure.

12.3 THE PAYMENT MECHANISMS

12.3.1 Token Based Payments

DigiCash has the potential to be one of the payment mechanisms that becomes a standard. However, issues raised in Chapter 10 did not necessarily raise answers that were acceptable. One of the biggest issues that DigiCash should face is the problem of private keys. The question of a bank's private key being found out has not been made an issue. The scenario of a private key being mislaid implies that the following are needed, if a token-based mechanism was to become the favoured on-line payment mechanism:

- Specific Issues of E-cash.

A specific issue of e-cash, each with its own key and each preferably secured in different places on different machines would bring some form of accountability to the company if a private key was discovered.

- Expiration Dates on Each Issue.

The shorter the lifetime of a key, the less time there is to hack a key by brute force and therefore there is less exposure to a broken key over time. Many international telephone companies put expiration dates on phone-cards. Although this is generally for accounting purposes, the theory remains the same.

- Competing Software Development.

By having many software companies developing different software, and the software being based on open protocols, then the effort required to hack the software is far outweighed by the amount of effort going in to building robust code.

With these three rules in place and with a full e-cash distribution, it can be seen to be highly unlikely to cause a major blackout of the payment mechanism at any given time.

12.3.2 Cash Based Payments

The main rival in the micro-payments arena to token-based payment methods are the cash-based payment systems. In previous chapters both have distinguished themselves in areas such as security, anonymity and the ability to make cost-effective low value transactions. However, the project has not really looked at the hardware that is a requirement to use a smart card based system. The companies Mondex, CAFE and Proton are not willing to give out technical details of their devices. Therefore it is necessary to form some basic rules and assumptions as to what an Internet compatible smart card device should be capable of. These features should be a feature of any smart card reader to be used for Internet commerce.

- Universal

  Devices should be compatible because the potential is there for usage by many different kinds of cards and software, at different locations, manufactured by different companies and so on.

- Cheap

  Because smart cards will keep on getting more complex, with operating systems potentially becoming as powerful as home computers. To enable low-value transactions to take place, the cost of the hardware must also remain low.

- Easy to use

  The card-reader must be as easy to use as perhaps a telephone or a remote control. To offer smart cards with more intelligent features should not imply that the usage of the device that reads the card should get harder.

- Time saving
  It has been explained that a transaction is quite complicated; the communication between two electronic purses goes back and forth, and various parts of the communication such as encryption and authentication are only done on the card. Therefore the interface must have the ability to process standard operations and send and receive data extremely fast.

Consumers may adopt smart cards because of their convenience. They are easy to carry and eliminate the need for verification of funds. The increase in security, the reduction in vandalism, the easy value transfer method all achieve great support from the merchant side of the equation. The additional cost of installing readers may be prohibitive.

A key issue with regard to true cash alternatives is that any contender that replicates the core features and benefits of cash is likely to achieve a number of goals:

- Recognisable
- Peer-to-peer Payments
- Unaccountable
- Immediate Value Transfer
- Multiple Currency Ability
- Reusability

For widespread acceptance the product should adopt a standard format that is familiar to consumers. Flexibility is added by allowing private person to person payments. As cash is unaccounted, acceptance will be aided by ensuring e-cash is unaccountable and the immediate transfer of value will aid cashflow within Internet business'. The ability to accept funds from all major markets or all countries provides sound reasoning for the need to have multiple currencies available from one 'purse'. Reusability is only an issue for customer convenience. The key point is that micro-payments should be readily available and acceptable anywhere for any payment.

12.3.3 Credit and Debit Card Payments

On-line credit card mechanisms provide no additional functionality to the payment system employed. CyberCash provides an 'envelope' with which to make secure on-line transactions. For credit and debit card transactions it is necessary to provide functionality over and above the basic requirements.

The ability to accrue transactions will enable users to make micro payments in a cost-effective and easy manner. There are two ways in which this could be handled. The first would be to settle transactions monthly so that users would know when they are going to be billed. However, if usage is infrequent and bills are low then this is not cost-effective in the same way that a single transaction is not cost effective. A second way would be to bill users when they accrue a certain amount of credit. This would ensure that billing only takes place when it needs to and that cost-effective thresholds are met.

Additionally, debit transactions have the potential to worry users because debits are taken directly from a bank account. To counter this it is recommended that debits are not taken directly from bank accounts

and that charge accounts are set up that delay the automatic payment from a bank account by including a 30-day check period that allows users to audit their bills before payment is made.

12.4 THE WORLD WIDE WEB

The prospect of Internet commerce is not wholly viable without the user-friendliness of the Web. However, during this project the Web's limitations have become apparent. The Web is essentially a glorified document viewer until the technology appears to allow it to evolve. The Web's limitations are more noticeable in applications that are fundamentally *outside* the world of documents, yet are *inside* the electronic commerce arena. Among these are the following findings:

- HTTP lacks the notion of a session as it is strictly single task orientated rather than conversation orientated. Although it is possible to build a session mechanism using scripts, HTTP itself does not currently provide this. However, this may improved in later versions of the HTML specification.

- HTML is based on a 'them' and 'us' scenario, where there is a client browser and a document that needs to be served. It may be that as a result of this, the browser lacks the interactivity that is needed to allow Internet commerce. Even though HTML allows forms, this is a very limited form of interactivity.

- If the amount of electronic commerce undertaken is going to grow then so is the function of the Web. Information s only obtained when it is explicitly asked for, rather than when it is needed. For this to change the notion of the web should switch from a 'pull' model to a 'push' model. An example of this is the ability to have news delivered to your screen which is offered by companies such as PointCast [POI]. This will allow for subscribing to information and services and receiving them as they come available.

It is also important to note that the Internet is largely insecure, although secure versions of several protocols are being considered and that most protocols also do not have quality-of-service guarantees. Other failings include the inability to locate resources when they are needed and the highly heterogeneous nature of the network.

12.5 FUTURE TRENDS

The Internet clearly poses a threat to the banking community. It is impossible to quantify the effect of digital cash on the way physical money is spent, but it is evident that banks cannot assume that it will not affect their current operations.

There are perhaps three potential scenarios that could happen:

The first issue is that the Internet provides an extremely easy and user-friendly way for customers to 'shop around'. By utilising search engines such as Yahoo! [YAH] and Alta Vista [ALT], customers will be able to ask the software companies to provide details of the best rates for car insurance, home insurance and savings. As the Internet is a global network, then fierce competition will bring down prices and at the same time enable electronic commerce to flourish.

Secondly, there is a distinct possibility of a multitude of electronic cash systems. This could potentially lead to a highly fragmented marketplace which hinders the growth and usage of such systems. It is evident that the Internet often spawns 'de facto standards'. If the payment system of choice on the Internet is not the same as the payment system of choice for the physical cash replacement then banks will be required to facilitate two different access methods for their accounts. As well as hindering the growth and usage this would also affect the costs of running electronic cash accounts.

In addition to this, there may be a value-gap between the two payment systems, with Internet cash not being of equal value to traditional cash (as it maybe issued by non-banks). With an electronic cash currency, customers may not care, as long as the tokens are transferable and valuable, such as Phonecards or British Airways Air Miles.

Third and finally, it can be seen that if an Internet Service Provider (ISP) bans a payment system from its Internet service, then any currency that was held by a user would be worthless. In this way, having customers with the right software to use a given service is no guarantee that they will use that service. The main access to electronic banking will undoubtedly be the desktop PC running Microsoft Windows, but there is no guarantee that a user's bank will be one approved by Microsoft. Evidently, if Microsoft choose to release their own currency it can be seen that it is not a good idea to have your major competitor controlling access to your customers.

Banks need to ensure that they are not cut off from their customers. The digital cash method used by most customers on the Internet will be the ones that their PC desktop gives the access to. By restricting choice, competition will be throttled and banks could end up as icons on a monitor: just an undifferentiated group of service providers controlled by the organisations who permit or prevent access.

12.6 CONCLUSIONS AND SUMMARY

This chapter has looked at some of the trends that can be expected in the next few years. It has looked at improvements that can be made to each payment model to allow the follow of funds to be more effective and efficient and to allay consumer fears of anonymity being lost and problems concerning payments.

The problems of the Web have been discussed with explicit references to some of the problems that can be associated with HyperText Mark-up Language. These include the lack of 'sessions' and the current inability to 'push' information to consumers rather than waiting for it to be requested.

The chapter concludes with three potential scenarios in to which the notion of electronic commerce can emerge. The scenarios concern different ways in which the customer has to interact with the merchant and the ways with which the market can become fragmented.

Like any new technology, it would be impractical to think of the status of electronic payments as clearly defined. The number of merchants accepting electronic cash number in the hundreds. Card based electronic cash projects have only been implemented in pilot projects in a handful of cities across the globe. Never the less the trends of modern commerce, driven by the inherent weaknesses of traditional payment systems, point to the eventual rise of electronic payments. Its just a matter of time...and spirit.

CHAPTER THIRTEEN

EVALUATION

13.1 INTRODUCTION AND SUMMARY OF TASKS

This chapter concludes the report. It includes a summary and evaluation of the project. Aspects of the report and its results are looked into, including to what extent the project objectives have been met. I have endeavoured to include full definitions of the problems that were encountered and how they were solved. I have also included details about why the final objective was not met.

This project has primarily been concerned with the research and evaluation of on-line Internet payment systems. In addition to the main objectives, a look at the future requirements for Internet commerce has been included.

The project preparation needed extensive initial planning. A rigorous but fair schedule was drawn up to identify timing requirements, along with a list of potential problems and their associated contingency plans. Examples of risks included the inability to get hold of research or the inability to use and test a given payment mechanism. Before the report could be started, in-depth and exhaustive research was performed to gain some insight into the theories and knowledge base of the electronic commerce area.

Once research began, it was imperative to have close contact with the companies and a continuous schedule of background reading. The nature of the project meant that it was important to read the majority of IT journals and magazines in case further research was investigated. For this reason, libraries were scoured for journals such as Scientific American and magazines such as Byte, as they both extensively favour articles connected to this subject.

As the project progressed it became evident that the learning curve was steep as I was required to understand peripheral subjects including cryptography, network security and banking. The amount of research was generally stable, although researching the multitude of payment systems available was very time consuming.

The research work concluded with extensive thought and hypothetical reasoning and testing of the systems. The ability to use two out of three of the researched systems ensured that the research was constructive and hands-on.

13.2 PROJECT MANAGEMENT AND PLANNING

The task of planning for the project involved:

- Producing a list of objectives necessary to carry out the project.
- Scheduling the objectives to ensure the overall aims could be met.
- Rescheduling tasks that could not be completed on schedule.
- Establishing milestones for the project.
- Production of a formal project plan.

The planning was a time-consuming but important stage of the project. Activities were scheduled to a demanding plan, with little time afforded to rescheduling or special situations. It was also important to include external problems that may affect the project, such as coursework and job interviews.

This method ensured that the workflow schedule was hardly compromised for the lifespan of the project. Monthly assessments and comparisons with the plan were made to ensure that the project was progressing in the right direction. It can be seen that if there were any unanticipated actions that needed to be taken or pieces of work that needed to be modified, it would always be highlighted in a monthly assessment.

The project was also part-managed by way of weekly meetings with my project supervisor, James Malcolm. I ensured that I attended the majority of meetings to discuss my progress. In this way, I could see that the project was moving forward and James could comment on whether it was progressing in the right direction or not. James also read early versions of the report, commenting on whether the content was acceptable.

A list of problems is discussed in the following section. However, there were no 'job-stoppers', so the need to use crisis response methods is arguable.

Although no particular project management strategy was taken, the tasks that were performed were generally common to any approach. The management tasks that were performed were undeniably time consuming but I believe that the indirect benefits helped to deliver an orderly and better planned project.

13.3 OBJECTIVE EVALUATION

The following examines the project according to the objectives. Included is an evaluation of the choice of making the objectives and to what extent they were met, as well as an insight of the project management.

OBJECTIVE	CHAPTERS
• Understand electronic commerce as a concept well enough to identify the key functions of a system and to model particular requirements.	Task met - Chapter 3 Task met - Chapter 4
• Identify the key requirements of a successful payment mechanism based on a full understanding of currently available mechanisms.	Task met - Chapter 4 Task met - Chapter 5 Task met - Chapter 6
• Evaluate mechanisms available against requirements assigned. Subject the results to real life paradigm comparison to learn core competencies.	Task met - Chapter 7 Task met - Chapter 8 Task met - Chapter 9 Task met - Chapter 10 Task met - Chapter 11
• Conclude on what makes a good system, which mechanisms serve a particular purpose well and the general direction of electronic commerce. Is it viable?	Task met - Chapter 11 Task met - Chapter 12
• Implement an electronic cash payment system.	Task not met

Table 7: Project Objectives - 8/11/1996

13.3.1 Evaluation of Objectives

The first four objectives were all eventually met. The fact that they were wholly suitable is testament to the fact that they were chosen after much thought into what a research report should accomplish.

Objective One was to understand the concept of digital cash and identify the functions. This task is wholly met and explained in the modelling of the three key mechanisms in Chapter 3. It was a conscious decision at this point to modify the objective so that 'key functions' of the systems could include a detailed examination of security. This is because security is the most important and visible benchmark that most users will judge a system on.

The second objective involved identifying key requirements. Again, this is wholly met with detailed analysis given into the payment systems that are currently available and a chapter devoted to mapping out key user requirements. It was perhaps too much to ask to 'identify key requirements based ... on a full understanding of current systems' as this implies that the full functionality of the nine evaluated systems should be examined. However, by gaining a full understanding of the systems available, I was able to get a better understanding of the workings of electronic commerce.

The third objective involved amalgamating the previous two objectives. The end results can be seen in Chapter 7. This part of the objective was completed successfully which meant that the second part of the objective could be examined. Whilst Chapter 7 broadly cross-references all the mechanisms against all the requirements, I felt that this was not investigative enough. Therefore I decided to modify the objective to allow an in-depth look at a few payment systems. The ideal situation of having three payment models in Chapter 3 meant that I could allow this objective to closely examine those three payment mechanisms. The results of which can be examined in Chapters 7, 8 and 9.

By way of having three in-depth examples, the ability to subject the results to 'real life paradigm comparison' was realised. The three hypothetical situations given in Chapter 11 successfully suited the objective. Therefore, the whole modified objective was completed.

Objective Four was the conclusion to the investigation and involved examining how well the systems provide their respective services. This objective was purposely vague to allow a myriad of comments and issues to be looked into. Chapter 11 'widens' this objective by looking into some of the particular problems that arose or could arise in the near future. None of the previous objectives wholly stated 'what are the problems?', so I felt that they could come under this one.

I also felt that that the 'general direction of electronic commerce' objective allowed me to look into the issues that needed to be addressed to allow commerce to prosper. This also involved 'expanding' the objective to allow an insight into both technical and idealist solutions that would benefit this area.

My advanced objective was not met. This was for four main reasons:
1. The amount of information and subjects to be examined was greater than I imagined, as was the scope of the subject area.
2. The ability to code a robust payment system has not yet been accomplished by a group of experts, let alone a single student and a project of this size would need to be taken as an entire dissertation.
3. The time taken to set up an information server, without coding would provide limted extra understanding of the subject area and would not provide any real 'deliverables'.
4. The amount of time available to code after research was completed was negligible.

I do not feel that this was an attainable requirement given the amount of work that was needed to deliver a report containing completed objectives 1 to 4. Given the option, I would have left the final objective out and devoted some more time to cryptographic and security research and included some metrics to evaluate the strength of each system.

13.3.2 Time Management

The project was aided by a proactive approach to research and writing. There were two possible ways of approaching the report and I chose to write up the report as I researched it, rather that completing all research and then writing up the results. In hindsight this was definitely the right approach, as it meant that my last 6 weeks were not tied up with continuous writing and trying to remember ideas that I established in the early weeks of the project. The plan was obviously suitable for my project objectives.

13.4 REPORT EVALUATION

13.4.1 The Objectives

The 'deliverable' part of the report contains information that satisfies the first four requirements of my objectives. Additional information contained within the project expands and builds on the objectives. The following analysis explains how the tasks were met and how decisions were made. An analysis and explanation of the objectives is in the previous section.

13.4.2 Chapter Two - Background Information

The first chapter of the report, Chapter 2, details some background information about electronic commerce. The key issue when writing this chapter was to decide how much information was needed to

explain what the Internet is and how companies are experimenting with it. After careful thought, the chapter was kept purposefully small, detailing enough information to allow the reader to understand the functionality of money and how commerce can be intertwined with technology. It was decided at this stage that although EDI forms an important part of the electronic commerce framework, it was not within the scope of the project. For this reason, a short list of the shortcomings of EDI is included to enable the reader to compare the systems that are investigated in the project with the systems that are presently in use today.

13.4.3 Chapter Three - Electronic Payment Mechanisms

For the benefit of the reader, the Electronic Payment Models chapter details the difference between micro- and macro-payments. Although not a key issue at this point, the ability to differentiate between small and large payments becomes a key feature further on in the project. Research into financial payment models provided three mechanisms to which I believed Internet payment models could successfully be mapped on to. At this stage, it was possible that there could be a fourth model based on a charge card scenario, with payments being accrued until a certain time period or value was reached. After careful consideration, I believed this to be too much of a niche model, and subsumed it into the credit/debit idea. Other considerations included a 'direct-debit' style model, but this failed as a result of its unaccountability to users, with funds being debited from an account before the amount of funds to be debited is approved. It can therefore be seen why there are three electronic models and not five.

13.4.4 Chapter Four - Security

It was decided to look at security in the next chapter for the simple reason that it is the most relevant issue to determine whether a system is safe. Again, it was important to communicate a great many complex ideas within one concise chapter. For this reason, only the three main cryptographic functions were investigated and examined, with each function measured against the main security uses needed for electronic commerce. The majority of diagrams were included after the text was written to aid the reader in understanding a very complex subject. The diagrams are not intended to replace the text, only to serve as a learning aid.

To ensure completeness, examples of alternate security approaches and systems were included to allow the reader to see that there is a gluttony of security systems available. The main problem of this chapter was deciding which measurables the three payment systems should be considered against. the resulting features were chosen because of their relevance to the commerce area and the needs of payment systems. It was decided not to include measurables such as speed of encryption/decryption as the systems are not like-for-like and it is already widely acknowledged that there is a trade-off between speed and strength of encryption and that a hash algorithm will always be the fastest but least secure cryptographic function.

The only other issue that was relevant was which 'other' systems and approaches were included towards the end of the chapter. It was decided to concentrate on the systems and approaches that are used in the systems that have not yet been commercially released. This goes some way towards 'future proofing' the research. The inclusion of PGP is as direct result of its popularity in the marketplace and its use in encrypting a great number of e-mails.

13.4.5 Chapter Five - Payment Systems

Chapter 5 was the easiest chapter to write but the hardest to research as there is great number of complete and uncompleted payment systems available on the Internet. To progress from a situation of having over twenty-five possible payment mechanisms to the nine that were summarised, it was necessary to set some criteria with which to measure each payment system against. The main criteria were whether the system was completed and usable and whether the system aligned with the 'models' given in Chapter 3. Minor issues such as the inability to access WWW homepages also reduced the list of payment systems to be evaluated.

The final nine systems were all researched with great detail to ensure that the understanding of their features was correct. The small size of the chapter belies the amount of time and research that went in to this section but underlines the importance of extracting only the correct information to present.

13.4.6 Chapter Six - Payment System Requirements

The shortest chapter looks at mapping out the key user requirements for a payment system. It was important to ensure that the requirements embodied functionality that every user could expect but at the same time was concise and relevant. To get to the final piece, it was necessary to draw up an exhaustive list of the functionality that any system could be expected to achieve. This was achieved by use of the brainstorming technique. A list of thirty requirements was reduced to twelve by way of establishing a ranking order based on the requirements of merchants, users and systems providers. An example of one of the requirements that was not used is that of divisibility, as it was not a key requirement for the system providers:

"Digital cash should be able to be subdivided into smaller pieces of cash. The cash must be fungible so that reasonable portions of change can be made. A user should be able to approach a provider and request digital cash breakdowns into the smallest possible units. The smaller the breakdown the better, to enable high quantities of small-value transactions."

It was felt that this was aimed too much at the token system and was not a requirement that had universal qualities. Another example that is mentioned in the text is the requirement for consumer protection.

13.4.7 Chapter Seven - Mechanisms Versus Requirements

This chapter was the next logical step for the project. It examines the interaction between the previous two chapters by researching whether the payment systems that had been studied earlier fared well against the requirements that a user needs.

The major obstacle for this chapter was how to present the results. It can be seen that the first table is presented with each individual system compared to each security requirement, whereas the remaining tables compare the requirements with each payment model. The reasoning behind this is that the security on each system can be differentiated from its competitors but the commercial requirements cannot be easily differentiated between systems that are based on the same payment model.

An alternate obstacle for this chapter was providing enough information to provide explanations for the tables but without giving away information that would be used to evaluate the payment mechanisms in the later chapters. It was decided to give only a brief overview of the results in this chapter and leave the extended detail for the relevant in-depth evaluations.

13.4.8 Chapters Eight, Nine and Ten - CyberCash, Mondex and DigiCash

My project plan for these chapters involved 'providing a clear and concise evaluation of the payment system, looking at their suitability as a payment system and the features that they provide to users and merchants'. It was firstly necessary to decide which payment systems should be looked at in-depth. The logical choice would be the best three systems, yet this implied that one or more of my models may not be represented. To this extent I decided to choose one example representing each of the models derived in Chapter 3.

Mondex was chosen because it is a British innovation and would therefore be easier to contact and its rivals did not appear to offer any English language information. Some notable rivals, including Proton of Belgium, did not even release enough information to allow them to be assessed in Chapter 5. DigiCash was chosen because it offered greater functionality and a more completed offering than its rivals. CyberCash was the hardest to select and its greater acceptability in the marketplace proved to be the decisive factor. It may have been easier to choose a Visa or Netscape-backed system as greater

research and documentation was available, but I felt that this defeated the purpose of the project of investigating the premier on-line payment systems.

The research for this chapter involved a logical extension of the early research that had commenced in Chapter 5. However, due to the amount of information needed it was necessary to devise a separate project plan to manage the information. I also contacted analysts at the companies involved and received useful information in return.

The key issue was divesting the information received of marketing speak and fanciful promises, whilst testing the ability of the mechanism to provide the services that are offered and meeting the requirements that had been previously established. I believe that the chapters were written containing the maximum amount of information in the minimum amount of text.

13.4.9 Chapter Eleven - Putting the Systems Into Practice

This is a logical extension to evaluating the three payment systems. The three preceding chapters evaluated the payment systems against my requirements. The aim of this chapter was to extend the evaluations by use of three hypothetical situations. The situations were especially designed to test as many aspects of the payment systems as were possible and to provide a broad example of the type of payments that a system could be expected to make.

It was decided at a late stage to include an analysis of the failures and the problems that could be associated with each system. The reason for including this analysis is to provide a counter-argument to the impact of electronic cash. The project is understandably very pro-electronic cash up to this point and I believe that the 'Analysis of Problems' section proves that there is a long list of issues that still need to be solved. It was also included to ensure that negative aspects of the systems were discussed and examined before conclusions were made.

13.4.10 Chapter Twelve - Future Trends in Electronic Commerce

The main reasoning behind this chapter was to provide an 'epilogue' to the research. My objectives stated that I should 'Comment on... the direction of electronic commerce' so I aimed to make a valued look into the failings of the systems that I had investigated in the belief that I could make some constructive suggestions as to how the situation could evolve. The suggestions were purposely taken from both technical and usable viewpoints to ensure that a true cross-section of ideas were presented.

An issue when writing this chapter was deciding whether ideas including the inability of the Internet to guarantee service levels should be noted. It was decided that in the interest of brevity and technical knowledge of the readership it was not necessary.

13.5 PROBLEMS ANALYSIS AND SOLUTIONS

Throughout the span of the project, it was evident that there would be many 'issues' regarding both the gathering of research and the writing of the final analysis. This section examines the problems associated with this paper and the solutions that were implemented in response.

13.5.1 Internet Access

As this project is based on on-line commerce, it was imperative to have fast access to the Internet. I was totally dependent on the Universities Internet link and this caused a problem. My project not only involved logging on to 'customer oriented' web sites (i.e. graphic intensive) but also downloading large software packages and researching world-wide electronic commerce Web sites. Access to this resource was very limited after 11:00 am, caused by a combination of an influx of students to the Computer Centre and the North American continent 'waking up'.

To counter this problem, I undertook to research from 8:00 until 11:00 every morning until that stage of the process was complete. I also worked on Weekends whenever was possible, as the network load was bearable if downloaded files were small.

13.5.2 Access to On-line Research.

There are many on-line resources that provide information and research pertaining to electronic commerce. The vast majority are concerned with the established EDI standards rather than future aspects of payment systems. It is also apparent that the few papers that are entitled 'Electronic Commerce' are more concerned with modelling systems to replace cash in 30 years time rather than concentrating on the technical aspects of the systems that will be used in the near-future.

My research therefore could not be information based and would have to entail evaluating actual systems. This was expected beforehand, but I did not think such a major percentage of the project would be based on hands-on research.

The helpful research that I downloaded was read and filed into specific folders, depending on the type of payment systems it looked into and the conclusions it came to. Examples of research can be taken from the Glossary. Most papers lacked in either depth or breadth of the research undertaken, but some introduced interesting issues.

13.5.3 Access to Printed Media and Research

The most striking problem that became evident was locating printed matter on the subject of electronic commerce. It was a task in itself finding references to reports and papers, but the lack of available information was surprising. An example of the problems that were encountered can be seen in the copy of my library record below. 'The British Library have informed us that they do not hold this item and are unable to trace it within the UK' was a phrase that I subsequently read over a dozen times.

- Jones, D. Smart Cards and the Internet. IN: Card Technology Today, 7, 2, September 1995
  Request made: 11:04 15-JAN-97 Number: 76610 Cancel after: 14-APR-97
  Awaiting reply/supply of item from REQUESTER

  29/1/97 The British Library have informed us that they do not hold this item and are unable to trace it within the UK.

- Ahuja, Vijay. Secure Commerce on the Internet. 1996?
  Request made: 10:11 31-JAN-97 Number: 77684 Cancel after: 14-APR-97
  Awaiting reply/supply of item from REQUESTER

  3/3/97 The Bodleian copy is in processing - they have asked us to retry in 8 weeks - do you wish us to retry?

- Kalakota, Ravi and Whinston, Andrew (Eds). Readings in Electronic Commerce. 1997
  Request made: 20:38 4-FEB-97 Number: 77994 Cancel after: 14-APR-97
  Awaiting reply/supply of item from BRITISH LIBRARY - ARTTEL

- Towards Electronic Commerce Cards on the Net. IN:World Card Technology, Feb/Mar 1995
  Request made: 19:47 4-FEB-97 Number: 79121 Cancel after: 14-APR-97
  Awaiting reply/supply of item from REQUESTER

  3/3/97 The British Library have informed us that they do not hold this item and are unable to trace it within the UK.

Source: libvax.herts.ac.uk

Figure 26: Listing of Library Requests

In light of this problem, I took a proactive approach and travelled to London to locate the books. Unfortunately, most bookshops stated that the majority of texts had not been released in the United Kingdom and that they would therefore not be able to get hold of them.

An alternative approach was to visit local libraries, but this turned out to be a waste of time and effort as they generally believed that the book would not warrant enough interest. Therefore this project was completed mostly without the help of printed media, and the impetus was focused on electronic media. This meant that the skill of information management was required and attained.

13.5.4 Understanding Cryptography

Cryptography is a technical subject that needs time to understand and master. My task was to fully understand the systems, their implementations and the ramifications of their use in a very short period and communicate this understanding to the reader.

The problem was that the subject area needs detailed explanations for a technical audience and explanations of the consequences and uses of each system within electronic commerce. The key to deciding which issues should be examined was to concentrate on the three main cryptographic functions, but also to examine a broad range of alternate security systems and approaches. In this way, an entire understanding of the subject is understood and presented.

13.5.5 Written Style

The key to completing this report successfully was the ability to avoid being repetitive wherever possible. Within the scope of this project it was possible to mention, for instance, Mondex's security in no less than 4 different chapters (5.2.1: Mondex, 7.1: Security Requirements, 9.4/5:Security Aspects/Mondex Evaluation, 11.1-6; Putting the Systems Into Practice). This pattern repeats itself for many issues. My project management plan ensured that when a topic was described in any depth, then the information was not repeated at a later stage of the project.

An alternate issue was that of being succinct. I have purposely kept the amount of text to the minimum that can successfully communicate the situations and ideas. The use of diagrams aids the text when it is needed and eliminates the need for further explanation of ideas.

Finally, the correct balance between explanation and evaluation was needed. It was necessary to have moderate usage of phrases such as 'it is evident that...', 'this implies...' and 'it can be seen that...' to ensure that the reader knows that the evaluations of the systems were not copied out of textbooks and are the authors own work.

13.6 SUMMARY AND FINAL STATEMENT

This chapter has evaluated many parts of the project. After a brief summary of the project the project evaluation has been described. The project, including each individual objective has been analysed. The objectives did change and an explanation for the change has been given. It is evident that the project management technique was sound but the objectives were perhaps too hard. It is also noted that a key hurdle to this project was obtaining and managing the information .

The report has successfully investigated the emerging area of electronic commerce. By investigating what requirements are needed and then looking at what requirements are actually delivered the report suprisingly concludes that DigiCash is currently best placed to deliver an on-line commerce solution. Its ability to work in many diverse situations means that it can potentially expand the marketplace for Internet transactions. The report produces evidence that there are still many obstacles to electronic commerce. However the need for a secure and reliable payments system keeps growing.

I am pleased to have had the benefit of a project that is forward-thinking in its nature and has the potential to be a real life requirement for the I.T. community and beyond.

BIBLIOGRAPHY

The following list of references is a summary of books and papers that have aided the research of this project. The items preceeded by an asterisk (*) are not directly referenced from the report but provide additional information on associated subjects.

ABA Advance Bank URL: http://www.advance.com.au/advance/ecash

ALA Lawrence, A. 1995 Publish and be robbed?, New Scientist, 18 Feb, 32-37.

ALV Alta Visa Search URL: http://www.altavista.com

AMX American Express URL: http://www.americanexpress.com

APA APACS July 1993

ARG Argos URL: http://www.itl.net/cgi-bin/argos/mainmenu

ASC Ascom URL: http://www.ascom.ch/systec/

BEL Bellovin, S. M. 1989. Security Problems in the TCP/IP Suite. Computer Communications Review. Volume 19(2), 32-48.

*BET Beth, Thomas. 1995. Confidential Communication on the Internet. Scientific American. Volume 273(6), 70-73.

BIR Birch, David G. W. 1994. Downloading Software, Uploading Money. In: Business on the Infobahn, Internet and the Enterprise, London.

BNK BankNet URL: http://www.mkn.co.uk/banknet

CHA Chaum, David. 1983. Blind Signatures for Untraceable Payments. In Advances in Cryptology: Proceedings of Crypto 82, Plenum Press.

CHB Chaum, David. 1992. Achieving Electronic Privacy. Scientific American. Volume 267, 96-101.

CHC Chaum, David. 1989. Unconditional Payer and Payee Untraceability. In Smartcard 2000: The Future of IC Cards. Edited by Chaum and Schaumuller-Bichl, North-Holland.

CIT CitiBank Thieves Transact $12M. [Online] URL:
http://www.itd.nrl.navy.ml/ITD/5540/ieee/cipher/news-items/old-news-items/950918.html
also:
Proactive Security and CitiBank [Online]
URL: http://www.bredex.de/EN/bredex/infos/security/V4.2/msg02711.html

CLA Clarke, G and Acey, M. 1995. Mondex Blows Users Anonymity. Network Week Oct 25.

COR Bell Communications Research: URL: http://www.bellcore.com/

CRY Schneier, Bruce. 1996. Applied Cryptography : Protocols, Algorithms and Source Code 2nd edition.

CYB Cybercash URL: http://www.cybercash.com

DBG Deutsche Bank URL: http://www.deutschebank.de

DES *Data Encryption Standard,* FIPS PUB 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

DIG Digicash URL: http://www.digicash.com

EAS Eastlake, D. et al. Credit Card Protocol Version 0.8 RFC 1898. [Online] Available FTP: src.doc.ic.ac.uk Directory: pub File: rfc1898.txt.gz

ECO Electronic Money. 1994. The Economist. Volume 333(7891), 25.

EPR DigiCash. Ecash Protocol Version 1.4. March 1996. [Online] URL: http://www.digicash.com/ecash/protocol.html

EUN EUnet URL: http://www.eunet.fi/ecash

EUP Report to the Council of the European Monetary Institute on Prepaid cards by the Working Group on EU Payment Systems. May 1994.

FLO Flohr, Udo. 1996. Electric Money. Byte Magazine, June 1996. Volume 21(6). 74-84.

FVH First Virtual Holdings URL: http://www.fv.com

GMR Goldwasser, S., Micali, S., Rackoff, C. 1982. The Knowledge Complexity of Interactive Proof Systems. In Proceedings of the 17th ACM Symposium on the Theory of Computing, 270-299.

GRA Grant, Mark. Reverend. (18 July 1995) Mondex. Cypherpunks Mailing List. [Online]. Available e-mail: cypherpunks@toad.com

HAR Harvey, Jack. 1988. Modern Economics, 5th Edition, MacMillan Education, London, p248

*HEL Hellman, Martin. 1979. The Mathematics of Public Key Cryptography. Scientific American. August 1979

INT Interlotto URL http://www.interlotto.li

KPS Kaufman, C., Perlman, R., Speciner, M. 1995. Network Security - Private Communication in a Public World. Englewood Cliffs, Prentice-Hall.

LAU Laufman, Steve. 1995. The Information Marketplace: Achieving success in Commercial Applications. In: Electronic Commerce. Current Applications and Issues. Edited by Adam, N and Yesha, Y. London . 1995.

LIF London International Financial Futures & Options Exchange URL: http://www.liffe.com

*LOS Loshin, Pete. 1996. Electronic Commerce: On-Line Ordering and Digital Money. Charles River Media, Massachussetts.

LLO Lloyd, P. et al. 1986. Introduction to Psychology - An Integrated Approach, Fontana, Chapter Eleven, p113-131.

MAI Crocker, D. 1982. Standard for the Format of ARPA Internet Text Messages. [Online] Available FTP: src.doc.ic.ac.uk Directory: pub File: rfc822.txt.gz

MAS Mastercard URL: http://www.mastercard.com

MAT Matonis, J. 1995. Digital Cash and Monetary Freedom [Online] URL:http://info.isoc.org/HMP/PAPER/136/html/paper.html

MDX Mondex URL: http://www.mondex.com

*MER Merckle, Ralph. 1990. A Certified Digital Signature. In: G.BRASSARD (Ed.) Proceedings of CRYPTO 89, Lecture Notes in Computer Science, Springer Verlag. 218-238.

MOO Moody, G. 1984. The Whole World in your Hands. Computer Weekly. 26 April. p34.

MTB Mark Twain Bank URL: http://www.marktwain.com/ecash.html

NEU Neumann, B. Clifford. 1995. Security, Payment and Privacy for Network Commerce. In: IEEE Journal on Selected Areas in Telecommunications. Volume 19(8). October 1995.

NIS NIST. 1992. Proposed Federal Information Processing Standard for Secure Hash Standard. *Federal Register*, Volume 57(21).

NOK Nokia Telecommunications The 9000 Communicator.
URL: http://www.nokia.com/com9000/9000n.html

PHO BT URL: http://www.bt.com/community/aged_and_disabled/service6.htm

RBR Retail Banking Research, January 1995. URL: http://www.rbrldn.demon.co.uk.

RIV Rivest, Ron. April 1992. The MD4 Message Digest Algorithm RFC 1320. [Online]
Available FTP: src.doc.ic.ac.uk Directory: pub File: rfc1320.txt.gz

RIW Rivest, Ron. April 1992. The MD5 Message Digest Algorithm RFC 1321. [Online]
Available FTP: src.doc.ic.ac.uk Directory: pub File: rfc1321.txt.gz

RSA RSA Data Security URL: http://www.rsa.com

*SCH Schiller. Jeffery. 1994. Kerberos - Secure Distributed Computing. Scientific American. November Edition.

SUR Thammasat University Electronic Cash Money Survey [Online]
URL: http://www.tu.ac.th/thammasat/part/money.survey.results

TES Tesco Stores URL: http://www.tesco.co.uk

TIM The Chips are down for Virtual Cash. The Times. 9 October 1996. 'Interface' section.

TJH Jones, Tim. 1996. The Future of Money. In: Submission to the US House of Representatives June 11.

TST Toxopeus, Jasper (Thursday 1 December 1996) Your ecash account [e-mail to James Mankin], [Online]. Available e-mail: jasper@digicash.com

USP Chaum, David. Blind Digital Signature Patent. US Patent Office.
U.S. Patent #4,759,063, July 1988 [Online]
URL: http://fetch.cnidr.org/cgi-bin/linker3?/pto7/NEW/INDEX+4759063+F

VIS Visa International URL: http://www.visa.com

VOK Voydock, V and Kent, S. 1983. Security mechanisms in high level protocols. In ACM Computing Surveys. Volume 15(2). 135-171.

WAY Wayner, Peter. 1996. Digital Cash - Commerce on the Net. Academic Press Limited, London.

YAH Yahoo! UK and Ireland. URL: http://www.yahoo.co.uk

APPENDIX A

SMART CARDS

A smart card is a small credit card-sized device that is able to handle substantial amounts of information. The main features of this information are that:

- it may be easily manipulated by an authorised user
- it is secure from unauthorised user

This is in direct contrast to a Compact Disc that is also small and can hold substantial data that is not manipulable. Data on a Compact Disc can not ever be erased. An audio tape is also small and can handle a great deal of data but it is not secure from unauthorised manipulation.

Current smart cards take the form of a plastic card with an embedded micro-processor, much like the phonecards that are used by BT [PHO]. The reason that they are a suitable mechanism is that they are cheap enough to allow mass distribution.

Smart cards can be used to hold any kind of information but their principal attraction in this area is the ability to serve a personal authorisation and recording devices for transactions. In this scenario a smart card can be referred to as an electronic-purse.

The use of a card is similar to those use in pre-paid schemes such as for photocopies in the library. A model of this situation would show an 'issuer' of the currency that is used in pre-authorised terminals until the value on the card has expired. The smart card improves on the situation by allowing varied transactions amounts as opposed to the static cost of copies. This is due to the smart card being able to hold more information.

Confidence is the key issue for a smart card issuer. The value stored on a smart card represents a liability of the issuer in favour of the user. There must be confidence that the liability can be met. This concern is shared by the Working Group of European Payment Systems who recommend that only institutions who are supervised by central banks or other authorities should be permitted to issue smart cards [EUP].

An alternative aspect of confidence is demonstrated in the integrity of the smart card itself. The possibility of unauthorised access to user details implies the ability to counterfeit virtual currency that would be difficult or impossible to detect given the assumption that peer-to-peer transactions are allowed.

By limiting the amount of transactions that a card makes or by limiting the amount of money available on a card would serve some protection against counterfeiting. An alternative route would be to monitor the activities of individual cards but this causes a user to lose anonymity. An audit trail of transactions can allow surveillance to take place.

APPENDIX B

SECURITY PROTOCOLS

Until recently, secure communications over the Internet directly implied that security was implemented at the application level, meaning that communications had to be protected explicitly by the user. This was generally in the form of encrypting e-mail.

S-HTTP, an extension of HTTP adds security below the application level. This is in comparison to the Secure Sockets Layer (SSL) which was proposed and implemented by Netscape and operates at the transport layer. This means that SSL can be used for private Internet transactions between systems and the programs that support it. The diagram below displays how the two solutions fit into the Internet data architecture:

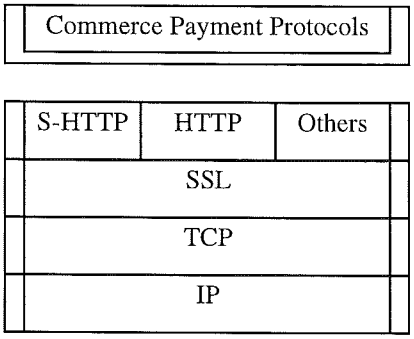


Figure 27: The Internet Data Architecture

S-HTTP adds security directly to the application, whereas SSL adds security to the entire data stream between the client and the server. This is because it operates above the transport layer. The fact that Internet security protocols can operate at different levels implies that they can all be used together if required.

B1. SECURE HTTP

Whereas HTTP defines the interaction between client and server and determines how the requirements are served, S-HTTP is a logical extension that determines the security aspects. The objective was to add security at the application level and add support for a range of security mechanisms. The protocol mechanisms include:

- Message Encryption
- Message Authentication
- Digital Signatures

Messages are used to negotiate between client and server. The protocols allows unprotected transactions as well as transactions including one or more of the above protection mechanisms. S-HTTP includes support for many cryptographic formats, including public and private key as well as key distribution schemes such as Kerberos. Each interaction between the client/server pair is negotiated to determine exactly what protocols are available and capable of being used.

S-HTTP encapsulates the HTTP interaction. This means that the data being transacted is contained within a special S-HTTP 'envelope'. It uses the same format as HTTP, indicating destination addresses and other information required by TCP/IP. As the data is encapsulated, the contents of the data to the network are irrelevant and intermediaries cannot know and do not need to know what is inside. Headers on the packets determine the correct addressing. The specification can be found (via FTP) at `ftp://ds.internic.net/`.

The header for S-HTTP requires two lines. The first identifies the type of content within the S-HTTP message ("Content-Type") and the second is the general cryptographic implementation being used ("Content-Privacy-Domain"). There are other optional headers that have the following uses:

- Indicating Data Representation of Enclosed Data
- Transaction of session keys and associated information
- Message Authentication Check which provides a message integrity check.

The message sent by S-HTTP can be simple HTTP data or another S-HTTP message. The contents of a message are interpreted by the receiving entity based on how the message is labelled and what kind of security treatment has been negotiated. S-HTTP also adds a set of security negotiation headers that are used to negotiate security issues. There are four separate issues which are negotiated between client and server:

1. Property - what kind of cryptographic options have been selected for a transaction.
2. Value - what specific implementation to apply to a system.
3. Direction - whether the negotiating system wants to receive security enhanced transactions or not.
4. Strength - how strongly the negotiating system wants an option from Yes/No/Optional.

This allows the two S-HTTP participants to negotiate secure transactions using cryptographic facilities that both client and server support and need.

B2. SECURE SOCKETS LAYER

SSL is different to S-HTTP as it requires the addition of an intermediate step before a network connection can be established. Data streams are encrypted before transmission and decrypted before they are used by the receiver. An advantage of this is that SSL can then be applied to any Internet application, not just the Web. A second advantage is that the resulting communications are reliable, private and authenticated.

An SSL session begins after the initiation of the TCP session. SSL links are initiated by a 'handshake' by which the two communicating systems exchange cryptographic information that will support the secure channel. Because SSL requires the use of TCP/IP, which also requires a three-way handshake, the server begins the session by waiting for the opening transmission from the client.

After receipt of an authentication message, the server responds with a randomly selected connection number and its digitally signed public key certificate. In response, the client sends off two messages in succession in the same way that TCP/IP closes a handshake.

The main similarity with S-HTTP is that SSL encapsulates the data. Subsequently it is held in an SSL record. The header to this record is small, with a length field and data pertaining to whether bit-stuffing has been used.

B3. INTEGRATING S-HTTP AND SSL INTO THE INTERNET

Special identifiers indicate which protocols need to be used to access a secure document. A normal WWW document would be fomed in this way: `http://www.herts.ac.uk/security.html`

The first part of the URL identifies the scheme that is used. To require S-HTTP to transmit a document, its URL must adhere to the form: `shttp://www.herts.ac.uk/security.html`

Documents requiring the browser to support SSL use the HTTPS scheme which should result in a URL that appears as: `https://www.herts.ac.uk/security.html`

It is important to note that the HTTP specification allows browsers to handle schemes that they don't wholly support. In theory, a non- S-HTTP browser would not be able to access any S-HTTP files, but will be able to handle HTTP files located on the same server.

APPENDIX C

GLOSSARY

ATM Automated Teller Machine - a cash dispenser as used by most banks.

BACS British Association of Clearing Services.
BellCore Bell Company Research - a leading telecommunications research company.
Browser Software that is used to search the World Wide Web.

CERN The European Particle Physics Laboratory based in Switzerland.
Ciphertext Text that has been **encrypted**. See plaintext.
Cryptography The study of mathematical process used for keeping data secret by **encryption**.

Decryption The method of turning **ciphertext** into **plaintext**.
DES Data Encryption Standard - a **private-key encryption** system.
DNS Domain Name System- a distributed database system linking host names to IP addresses

ECU European Currency Unit.
EDI Electronic Data Interchange - a method of making inter-company payments and invoices
EEPROM Electronically Erasable Programmable Read Only Memory as used in **smart cards**.
EFT Electronic Funds Transfer - a method of making interbank payments.
Encryption The method of turning **plaintext** into **ciphertext** using mathematical algorithms.

Finger A **TCP/IP** application used for retrieving information about a system or its users.
Firewall Hardware or software to prevent attacks on a network originating from the **Internet**.
FTP File Transfer Protocol - a protocol for transferring files across a network.

GUI Graphical User Interface - the 'front-end' of a piece of software.

HTML HyperText Mark-up Language - a subset of SGML that is used for writing Web pages.
HTTP HyperText Transfer Protocol - the transfer protocol for Web pages. See **WWW**.

IBM International Business Machines - American computer company.
IDEA International Data Encryption Algorithm. A block **encryption** algorithm.
internet A network of networks.
Internet The international network of networks that currently spans the globe.
IP Internet Protocol. Defines the interaction between hosts across an **internet**.

Kerberos A method if mediating the exchange of **keys** between users and hosts.
Key A quantity of data used to **encrypt**, **decrypt** or authenticate data.

LAN Local Area Network. A collection of computers in the same area on a single network.
LIFFE The London International Financial Futures and Options Exchange.

M0 A measurement of the physical money in circulation in the United Kingdom, See **M4**.
M4 A measurement of all money in circulation in the United Kingdom. See **M0**.
MDx Message Digest x - an efficient way of security by using a hash function. See **SHA**.
MIME Multipurpose Internet Mail Extensions - An e-mail protocol for non-text files.
MIP Millions Instructions per Second. A measurement for the speed of a microchip.
MIT Massachusetts Institute of Technology - the leading IT research College.
Multicast The delivering of information from one source to many selected destinations.

NCSA National Centre for Supercomputing Applications - the inventors of Mosaic **browser**.
NIST National Institute for Science and Technology (United States).

PGP	Pretty Good Privacy - an **encryption** program that utilises **IDEA**.
PIN	Personal Identification Number - a code that successfully identifies the user.
Ping	Packet Internet Groper. An application to determine if the remote host is reachable.
Plaintext	Text that has not been subject to cryptography. See Ciphertext.
Private-Key	**Encryption** and **decryption** of a message by use of a 'secret' key. See **Public-Key**
Public-Key	**Encryption** of a message using one key. **Decryption** by use of another.
RFC	Request for Comments - the precursor document to becoming an Internet standard.
RSA	Rivest, Shamir and Adlemen - a **public-key encryption** method.
SHA	Secure Hash Algorithm - An algorithm favoured by **NIST** incorporating **MD5**.
SHTTP	Secure **HTTP**. A secure form of the protocol implemented within the **browser**.
Smart card	A card that contains readable and writeable memory.
SMPS	Secure Merchant Payment System-interface between a Web server & CyberCash wallet.
SMTP	Simple Mail Transfer Protocol - the favoured **Internet** mail delivery solution.
TCP	Transmission Control Protocol. A reliable communications protocol.
Telnet	A program for connecting to remote computers.
URL	Uniform Resource Locator. A protocol for defining the location of a **WWW** resource.
VTP	Value Transfer Protocol. Security protocol as used in the Mondex system.
WWW	The World Wide Web.