Université d'Ottawa · University of Ottawa

# Université d'Ottawa · University of Ottawa

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES

FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

Pramav SHARMA

AUTEUR DE LA THÈSE - AUTHOR OF THESIS

M. Sc. (Systems Science)

GRADE - DEGREE

Systems Science Program

FACULTÉ, ÉCOLE, DÉPARTEMENT - FACULTY, SCHOOL, DEPARTMENT

TITRE DE LA THÈSE - TITLE OF THE THESIS

An Evaluation of E-payment Systems and their Application in Mobile Commerce

D. Wright

DIRECTEUR DE LA THÈSE - THESIS SUPERVISOR

CO-DIRECTEUR DE LA THÈSE - THESIS CO-SUPERVISOR

EXAMINATEURS DE LA THÈSE - THESIS EXAMINERS

M. Benyoucef

J. Nash

J.-M. De Koninck, Ph.D.

LE DOYEN DE LA FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES

DEAN OF THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

# University of Ottawa

## Master's Program in Systems Science

## Thesis

**An Evaluation of E-Payment Systems and Their Application in Mobile Commerce**

**Student Name: Pranav Sharma**

**Student Number: 2411937**

**Thesis Director: Professor David Wright**

**Faculty Graduate and Postdoctoral Studies**

**University of Ottawa**

**December 13, 2004**

*Your file Votre référence*
*ISBN: 0-494-01604-3*
*Our file Notre référence*
*ISBN: 0-494-01604-3*

# Abstract

Electronic commerce is growing at an ever increasing pace every year. However, the payment mechanisms in use were developed without electronic commerce in mind, and as a result, must be modified before they may be used for online transactions. In this thesis, the online payment mechanisms in use are analyzed to find out if they meet present day electronic businesses requirements. A comparative study of existing payment mechanisms has been performed and their strengths and weaknesses evaluated. Recommendations are made for improved mechanisms capable of meeting the needs of consumers and businesses today.

# Acknowledgement

I wish to thank Prof. David Wright for his support, guidance and inspiration both as a supervisor and as a teacher. I wish to convey my thanks to those people whose work have been referred to in this thesis and have inspired me.

I would also like to thank the departmental staff for their kind help and for offering me, the resources I needed.

I wish to express my thanks to the Faculty of Postgraduate and Doctoral Studies, University of Ottawa for their support.

Finally, I wish also to thank my family for their continuing support throughout this work.

# ---------Table of Contents---------

# ---------List of Figures----------

# ---------List of Tables---------

# Chapter 1 Introduction

Initially, the Internet was used primarily as a medium of information or advertising. For many years, people purchased products online using traditional means of payment, writing a cheque or money order or paying cash at a retailer. With the growth of Internet and electronic commerce, there is an immediate need for a new comprehensive electronic payment system. However, the development of a new payment system lagged behind because of issues such as liability, integrity, trust and identity. In this thesis, we will be focusing on "Electronic Money" and we will discuss these issues as we go.

## 1.1 Why Electronic Money?

According to an article published in IEEE Spectrum by Kelly [1], money fulfills three social functions. First, money is a way to measure and record value. Second, it can be used to store value conveniently for future use. Third, money represents a medium of exchange. In order to fulfill these functions, money has to satisfy several requirements: broad acceptability, being difficult to fake (counterfeit), having guaranteed value, and being inexpensive and convenient to use.

There are many payment instruments that can fulfill these requirements, for example, paper and coin cash, debit and credit cards, and cheques. These instruments are broadly accepted and they can be considered as traditional means of payment.

According to the latest figures from the Statistical Abstract of The United States, 2001, based on the number of transactions, even today about 42% of transactions use cash. The reason behind the popularity of cash is that it is portable, requires no authentication, and provides instant purchasing power. Cash allows for micropayments. The use of cash is "free" in that neither merchants nor consumers pay a transaction fee for using it. Using cash does not require any complementary assets, such as special hardware or the existence of an account, and it puts very low cognitive demands on the user. Cash is anonymous and difficult to trace, and in that sense, it

is "private." Other forms of payment require significant use of third parties and leave an extensive digital or paper trail. Beside cash, personal cheques, credit cards, debit and other cards are also popular. Why do we need a new form of money, electronic money?

Traditional payment instruments are convenient for face-to-face interactions, where the payer and the payee have the possibility of direct contact. However, they are not suitable in remote transactions where there is no possibility of direct contact between the payer and payee. There are several examples of applications where remote interactions are the basis of the payment transaction (e.g. electronic commerce over the Internet, Electronic Fee Collection). Moreover, with advances in wireless and mobile technologies, new payment schemes are being introduced where products and services can be purchased remotely.

On April 23, 2003, EMI Record Music announced its plans for the biggest European music download initiative to date, via a record company in Europe. The company makes available for sale online over 140,000 tracks from over 3,000 EMI artists. Similarly, other music companies such as Sony and Universal have plans of their own. Typically, the songs cost $0.99 USD or more. The users have various options to pay for the songs, including electronic money. New types of online information products (such as sports scores, news flashes and weather reports) require micropayments. All of these new developments call for a new form of payment that can be used for online shopping as well as for creating enhancements to existing systems.

Electronic Funds Transfer (online banking or Credit card) can be used for remote payments transactions in which the payer and the payee have already established a contract describing their business relationship. The payment of bills for electricity and gas are examples. However, Electronic Fund Transfer is not very effective when the payer and the payee have not regulated their business relationship by means of an underlying contract. Also, by using Electronic Fund Transfer, the payer reveals his or her identity, and this raises the question of privacy.

Electronic money is easy to issue, circulate, and store, which make it attractive even for payment transactions based on face-to-face interaction. A smart card can be used by a payer to make small payment to vending machines, to pay for the weekly shopping in a supermarket, or to a pay bill

in a restaurant. The card can then be recharged with any appropriate currency (for international travelers) at the bank or at an ATM (Automated Teller Machine) or on a smart card reader connected to a PC at home. The issuing of electronic money does not involve a printing machine with special characters, ink, or paper. Electronic money does not deteriorate during circulation. The participants do not need safe-deposit boxes to store or transport it.

One of the most important arguments in favor of electronic money is the convenience of use to both the payer and the payee. For consumers, this will consist, among other things, of ease in obtaining cards and replenishing them, as well as plenty of opportunities to use them. Merchants will want to see fast and easy service requirement on the part of their staff and fast settlement of the amounts due to them.

At the same time, we should also note some issues with electronic money. First, it is worth considering the integrity issue. Electronic money is finally just a string of bits. It is just sufficient to record a bit-string representation of electronic money, and then to forward it a second time to a merchant. This can happen when an eavesdropper "listens" to financial information sent on the Internet (such as the account number of a credit card) and uses this information for ordering purchases on behalf of the cardholder. It is also very tempting to try to forge electronic money in an undetectable way. Therefore, it should be possible to distinguish between a bit-string that represents a value and a representation that bears no value. These are just two threats that relate to the integrity of electronic money. Unlike paper currency, trust is also a very important issue when it comes to electronic currency. When the payer and payee are relatively unknown to each other and are well beyond their geographical boundary, trust becomes an important question. Privacy is also a potentially sensitive issue. Payers may wish the content of their transactions to be kept private. In this case, it is normal that they not want neither the shop to be able to read their identity from the electronic money, or for the issuer to know where a specific sum of money was spent. At the same time, the payees and issuers may require that the content of transactions be captured in appropriate records in order to prevent fraud of one against the other.

An electronic payment system is a set of participants, and their interactions towards an efficient exchange of value among them, using electronic money as the payment instrument. The

interactions include the issuance of money, use of money, storage of money, and the clearing and settlement of financial operations. The main obstacle to worldwide acceptance of electronic money is ensuring the integrity and privacy of all the participants.

According to Canadian privacy laws[2], "an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (c.1), made to a government institution or part of government institution that has made a request for the information and identified its lawful authority to obtain the information, or (2), made on the initiative of the organization to an investigative body, a government institution, or a part of a government institution and the organization." Thus, law enforcement authorities may use this bill to obtain relevant private information from the bank concerning an individual.

This raises an issue of conflict of interest: while we as users want total privacy and no paper trail and want to be anonymous, the financial institutions and banks want to have records for law enforcement authorities. We will have to address these questions before the electronic money goes into usage.

## 1.2 Outline of the Thesis

The thesis comprises six chapters including summary and conclusions. Towards the end, we have added a detailed description in the appendix. The chapters are organized as follows.

The first chapter introduces the thesis topic and stresses the need for electronic money. We try to give a brief history of its evolution. We will present the ever-shifting market trends related to e-commerce. We will introduce our objectives and methodology and explain our evaluative criteria's. The second chapter presents a background of the traditional payment systems. It talks about the most widely used payments systems. We talk about the shortcomings in the systems and sheds light on its brief historical preview. We then talk about the electronic payment system framework and lay down the norms for a successful electronic payment system.

The third chapter introduces various electronic payment mechanisms. It gives a brief description of their operation. The detailed explanations can be found on the appendix.

The fourth chapter presents our results and analysis. It rates the payment systems and justifies its ratings on concluding pages. We divided the table into two parts, one that compares "Digital Cash," "Electronic Cheques," and "Credit cards," and one that compares "Smart cards" to "other form of online payment mechanisms."

The fifth chapter summarizes and concludes our findings and ends with recommendations for the improvements for their future use.

The first appendix addresses the encryption and cryptography used in payment system. We introduce the various encryption technologies. We also talk about digital certificates and their management.

The second appendix talks about electronic cash (E-Cash) and introduces its advantages. After briefly explaining the way E-Cash works, we discuss two products, namely, "NetCash" and "Ecash." At the end, we analyze NetCash and Ecash, and the strengths and weaknesses of electronic cash payment systems are compared.

The third appendix takes up electronic cheques. After giving a brief model of their working, along with their popularity, we give examples of three electronic cheque systems, namely, "NetCheque," "CheckFree" and "NetChex." The chapter explains the working of the electronic cheques and then evaluates them. At the end, an analysis is carried out we tabulate the strengths and weaknesses of electronic cheque payment systems.

The fourth appendix focuses on smart cards. After giving a brief history of their evolution, we talk about various types of smart cards, namely, "contact," "contact less," "hybrid," "memory" and "microprocessor." We then take up the standards that are in place for smart cards, and analyze two examples, "Blue" from American express, and "Multos 4" from Gemplus. Chapter 6 also focuses on the smart cards that can be used for retail business, such as prepaid cards, also

known as "stand-alone smart cards." We then compare the advantages and disadvantages of stand-alone smart cards compared to authorization-based smart cards. The chapter ends by talking about future trends.

The fifth appendix introduces credit cards. After introducing the history and advantages offered by the cards, we focus on the security protocols used in credit cards, namely, "Secure electronic transactions" (SET), and "Secure socket layer" (SSL). We discuss Secure Socket Layer (SSL) in detail, since it is the *de facto* secure protocol for e-commerce and wireless transactions today. SSL does not provide mechanisms for handling payments, but it does offer confidentiality in Web sessions and authentication of Web Servers, and, optionally, of end users too.

We will also include in our discussion a new protocol developed entirely for payment cards, namely Secure Electronic Transactions (SET). It is not a general payment model; it is rather restricted to payment cards or similar applications in which, parties take on the role of buyer, merchant, or acquirer. It does not address transfer of funds from one individual to another and instead relies on the existing credit card infrastructure to effect the payment. We will analyze the two security protocols namely, "SET" and "SSL," and we end the chapter by highlighting the strengths and weaknesses of each.

The sixth appendix talks about the new mechanisms of online payment that are being currently introduced in the market, namely, "online banking using an ATM card reader", "e-mail money transfer", and "charging directly to the phone bill". The chapter briefly introduces the mechanisms and then synthesizes them. The chapter ends by comparing the strengths and weaknesses offered by each.

The seventh appendix focuses on mobile commerce payment systems. We introduce the various technologies involved to facilitate the payment systems that are widely used in securing Web-based transactions on wireless networks. We compare the two networks that facilitate the wireless data access in mobile devices namely, "Wireless Application Protocol (WAP)", "i-mode". We also analyze the two billings approaches prevalent in mobile data transfers namely, "content based" and "flat rate".

We study the security offered by WAP. WAP bridges the gap between the mobile world and the Internet as well as corporate intranets, and offers the ability to deliver an unlimited range of mobile value-added services to subscribers--independent of their network, bearer, and terminal. WAP uses Internet standards such as XML. Many of the protocols are based on Internet standards such as hypertext transfer protocol (HTTP) and TLS, but have been optimized for the unique constraints of wireless environment: low bandwidth, high latency, and less connection stability.

The eighth appendix provides some case examples where the use of E-payments systems more beneficial than conventional payments systems. The case examples refer to the real life situations where one might find using E-payment systems more suited than traditional ones.

## 1.3 Objectives and Methodology

The objective of the thesis is to determine if the most widely used online payment mechanisms meet the requirements of consumers and businesses. We also examine how the mechanisms fare when used for mobile commerce.

The methodology we adopt is an evaluative one. The evaluative criteria are based on our assessment of the most important needs and concerns of consumers and businesses. From the consumers prospective, the desirable properties for electronic payment systems are security, convenience, privacy, anonymity, immediate payment and remote access. These criteria's have been used by researchers and developers (Jayawardhena and Foley 1998 [3], Neuman and Medvinsk, 1995 [4]) develop and evaluate payment systems. With the increasing use of mobile communications, it becomes necessary to analyze the suitability of these payment systems for mobile commerce as well. Furthermore, a successful payment system also needs to take into account technical and implementation issues and issues of the concern of business community. Thus, we have analyzed the systems from business, technical and implementation point of view as well.

We will explain these criteria's in detail as follows:

Convenience

An electronic payment system must provide an edge over other payment systems in certain circumstances. There must be circumstances when the user finds it more desirable and convenient to use. The payment system should provide benefits over the conventional payment systems.

Security

Since payments involve money, payment systems should be secure, making it impossible for any hacker or criminal to attack. Since Internet services are provided today on networks that are relatively open, the infrastructure supporting electronic commerce must be usable and resistant to attack in an environment where eavesdropping and modification of messages is easy. We will evaluate security based on both consumer and on business view.

Privacy

Any personal information collected, must be done with the consent of the parties involved and should be used for a reasonable purpose. It should be ensured that that the information is stored and transmitted securely. Also, it should be used for the purpose it was collected (PIPEDA [2]).

Versatility

The system should be versatile enough to accommodate all the changes in technology and upgradeable from time to time. This means that it should not only be compatible with all the available machines and platforms but also have an allowance for future systems and devices. Versatility of the system also reflects the popularity of the system.

Acceptance by all parties

The usefulness of a payment mechanism is dependent upon what one can buy with it. Thus, a payment instrument must be accepted widely. Where payment

mechanisms are supported by multiple platforms, users of one platform must be able to transact business with users of other platforms.

Technical issues

The acceptability of a payment mechanism is affected by the trust in the system. The trust can be built up by demonstrating strong technical features. The technical features include "independence of operators" and "use of existing standards." By independence of operators, we mean there should be no third party involved in assuring the authenticity of the currency. The existing standard makes the mechanism easy to integrate with the devices and hardware. Technical features play a pivotal role in the popularity of the mechanism.

Implementation Issues

The implementation issues include "cost factor" and "speed to the market." The cost factor includes the cost incurred by the businesses or by consumers to use the system. This may involve buying new hardware or deploying a new system or training employees in using the system. Clearly, the chance of a system that has a very low benefit to cost ratio being successful in the market is very low. Speed to market is the time it will take for a new system to be completely absorbed and implemented in the market. If the system requires lots of additional hardware or specialized support systems and is complicated to use, it takes a long time to implement.

Traceability

To ensure the authenticity of the payment, some of the online payment systems need the feature of traceability. The traceability feature enables banks or issuers to confirm whether the consumer originally issued the payment. The law enforcement authorities enforce this feature. However, it should not be used as a violation of consumer privacy and should only be exercised by appropriate authorities.

Immediate payment

An online payment system should be in real time for both payee and payer. This becomes an essential criterion when the payment system is used for stock trades and auctions where money is exchanged several times during the day.

Applications in mobile commerce

Mobile commerce is an emerging field. Payment systems are still emerging for mobile commerce and even today standards are being set. One distinct advantage that mobile phones have over the wired networks is security.

Many phones that are used across the world are based on or support Global System for Mobiles (GSM), so users can take advantage of the unique security features offered by that technology. Each GSM device contains a personality device called a Subscriber Identity Module (SIM). This card securely holds the encrypted information of the identity of the customer. When the user inserts the SIM card into a phone handset and enters the appropriate PIN, the SIM card activates, authenticates itself to the cellular network, and negotiates a session key that is used to encrypt the content of traffic traveling over the air from then on. This authentication can be very useful in making payments.

For mobile commerce to be widely accepted, it needs to build on established habits, practices, and infrastructure, and then add specific mobility value. The added value can be, for instance, instant access and delivery, flexibility, convenience, personalization, location awareness, or better customer service. The key drivers of mobile commerce service adoption are ease-of-use and convenience, keeping the issue of security in mind. Applications and services that are too complex and time-consuming will discourage consumers from "going mobile." The challenge is to implement a secure payment scheme so that it remains convenient and simple to use.

Remote access

The payment mechanism should possess the ability to allow users to make payments from different locations with a range of interface devices. Users should be able to monitor their spending without going out of their way to do so.

We tabulate our assessment and grade the suitability of each payment mechanism each criterion. We have graded them based on our scale with five stars being the most acceptable and one star being the least. We summarize our findings in our conclusion and go over them in detail.

# Chapter 2 Payment Systems Introduction

A payment system is a set of participants and their interactions toward an efficient exchange of value between them. The interactions include the complete process of issuing and using payment, as well as the clearing and settlement of financial operations. Both participants and interactions are determined largely by the specific payment method that is adopted in the system. In the simplest scenario, the participants in a payment system can be considered in connection with three essential roles: the issuer of the payment means, the payer, and the payee.

In order to understand e-commerce payment systems, we first need to be familiar with the various types of generic payment systems. Then we will be able to clarify the different requirement that e-payment systems must meet and identify the opportunities provided by e-commerce technology for developing new types of payment systems. Some of the widely used models based on the above-mentioned systems are discussed below.

## 2.1 Types of Payment Systems

### *2.1.1 Cash*

Cash, which is a legal tender defined by a national authority to represent value, is the most common form of payment in terms of number of transactions. Cash has been in circulation for the longest time. The Federal Reserve Bank of New York estimates that about $675 billion of U.S. currency is in circulation [5].

The key feature of cash is that it is instantly convertible into other forms of value without the intermediation of any other institution. It is portable, requires no authentication, and provides instant purchasing power for those who possess it.

One distinct advantage of cash is that neither merchants nor customers pay transaction fees for using it. Using cash does not require any complementary assets, such as special hardware or the existence of an account, and it puts very low cognitive demands on the user. Cash is anonymous

and difficult to trace, and in that sense, it is "private." Other forms of payment require significant use of third parties and leave an extensive digital or paper trail.

`However, cash has its own problems. According to Federal Reserve Bank of New York publication (December,2002) [5], the life expectancy of a 1-dollar bill before it wears out is about 18 months and of a 50 and 100 dollar bill is about nine years.

Each bill costs about 4 cents to produce, varying slightly according to the denomination. This cost is ultimately borne by taxpayers. A similar situation exists in every country in the world. Nevertheless, cash is the most commonly used form of payment, accounting for about 80 percent of all transactions worldwide.

One of the factors that has allowed cash to remain the dominant form of payment is the development and use of the automated teller machine (ATMs), which allow consumers much easier access to money in cash form.

### *2.1.2 Payment by Banks*

When both parties lodge their cash in the bank for safekeeping, it becomes unnecessary for the payer to withdraw bills in order to make a payment to a payee. Instead, he can write a cheque, which is an order to their bank specifying the amount of money to be transferred from the payers account to the payee account.

#### *2.1.2.1 Payment by cheque*

Chequing transfers are funds transferred directly via a signed draft or cheque from a consumer's account to a merchant or other individual account. Cheques can be used for both small and large transactions, although typically they are not used for micropayments. Cheques have some float (the time interval between the deposit of the check in the bank and its payment), and unspent balances can earn interest.

However, cheques are not anonymous and require third-party institutions to operate. Cheques also introduce security risks for merchants. They can be forged more easily than cash; hence,

authentication becomes a necessity. Cheques can also be an additional risk to merchants as they can be canceled before they clear the account or they may be rejected if, there is not enough money in the account.

These so-called returned items are the major problem with cheques as a payment instrument, in that their existence introduces uncertainty, and the fact that they need individual attention from banking staff means that they require an expensive process.

Insured cheques reduce the security risks associated with personal cheques by requiring an up-front payment to a trusted third party: a bank or money transfer company such as American Express, Wells Fargo, or Western Union. These trusted third parties then issue a guaranteed payment draft called a money order that is as good as cash, although less anonymous. Merchants are guaranteed the funds in any transaction with an insured cheque.

Insured cheques provide merchants with lower risk, but they do add costs for the consumer. In return, consumers have a payment instrument that is accepted nearly everywhere and in some cases is insured against loss.

### *2.1.2.2 Payment by Giro or Credit transfer*

The returned items problem is the single biggest drawback with cheques as a payment method. In total, nearly twenty-nine billion cheques were written [6] in the US alone, in 2002. However, the projected numbers of cheques written in the year 2005 is twenty-eight billion. This decline is due to a shift in the personal sector as customers use credit cards in retailers instead of cheques.

Cheques payments have been falling by a billion (number of transactions) [6] every year and the trend is expected to continue, with the decrease in usage in cheques the cost of the return items that the customers have to bear becomes quite substantial.

This problem is eliminated using a credit transfer or giro payment. The processing of a giro is similar to cheques, with the main difference being that the transaction cannot be initiated unless

there are funds in the account. This eliminates any uncertainty and extra cost imposed by the need to process returned items.

### 2.1.2.3 Automated clearing house (ACH) payments

From their inception, paper-based payments (cheques and giros) have grown in popularity and as the task of carrying out paper-based clearing grew, the banks began to look for more automated ways to make payments. In 1968, a group of California bankers came together to form the Special Committee On Paperless Entries (Scope), which led to the formation in 1972 of the California Clearing House Association, the first regional automated clearing house (ACH) in the United States. In the UK, similar moves were happening, and an automated clearing center was established in 1968, which was incorporated in 1971 as Bankers Automated Clearing Services (BACS).

The ACH system operates in a similar way to that of paper clearing except that the payment instructions are in electronic form. The message has changed from a propriety format to a format that complies with open standards defined by the electronic data interchange (EDI) community.

In the United States alone, the number of ACH payments by financial institutions increased to 8.05 billion in 2002, up 13.6 % from 2001. These payments were valued at $21.7 trillion. Including payments originated by the Federal government, there were a total of 8.94 billion ACH payments in 2002 worth more than $24.4 trillion [7].

ACH payments include direct deposit of payroll, Social Security benefits and tax refunds, direct payment of consumer bills, business-to-business payments, federal tax payments, and increasingly, e-cheques payments.

### 2.1.2.4 Wire Transfers

The ACH method of effecting payments is ideal for mid-to-low-value transactions. In the United States, the Federal Reserve operates the Fedwire payment system, and a private organization called the Clearing House Interbank Payments System (CHIPS) is also in operation. Typically, these payment systems handle payments between corporations and banks, to, and from government.

CHIPS [8] is the largest bank-owned, privately operated, real-time final settlement payments system for business-to-business transactions. CHIPS pride itself on being the only system with real-time netting and built-in EDI (Electronic data interchange). It offers a variety of commercial payment capabilities such as:

- Matching capability: An algorithm for multi-lateral netting continually offsets and settles payments throughout the day. Payments are matched, netted, and settled usually in seconds. This allows payments to flow faster and maximizes liquidity.
- Real-Time Settlement: All payments are final upon release, and are assured by CHIPS to a participant bank.
- Straight-Through Processing: 93% of all payments are processed by CHIPS receiving banks without any manual intervention. This results in automatic posting, immediate notification and faster availability of funds.
- Universal Identifier Database (UID): This extensive, daily-updated database quickly and accurately verifies and matches corporate customers with their bank account information. With this unique feature, we only need to pass on our bank and UID number to process any transaction.
- Electronic data interchange: It provides corporate customers with the remittance details they need-customer numbers, invoice numbers, discounts taken and more--together with each electronic payments. This results in reduced errors and speedy reconciliation.
- Reliability: It claims to be 99.99% reliable.

CHIPS have multiple computers at its primary center and an identical system for backup at a separate center, ensuring its continuous operation and reducing operational risks. It also employs

a full payments-message authentication. This process authenticates the sender of the message and verifies that the information received has not been altered either intentionally or accidentally.

In the US, in the year 2002 the total dollar amount spent was $315,708,517,978 and the total number of transactions was 63,297,834 [9]. The average dollar amount per payments was $5,072 and average daily dollar amount was $1,257,802,860.

Similarly, in the United Kingdom, CHAPS (Clearing House Automated Payment System) which is an electronic transfer system for sending real-time gross settlement same-day value payments from bank to bank, handles the main high-value payment system. It is operated by the CHAPS Clearing Company, in partnership with the Bank of England, which provides the payment and settlements services. Following a strategic review in 1999, the CHAPS Clearing Company agreed to the development of New CHAPS. New CHAPS includes the migration from proprietary standards and networks to more generic SWIFT (Society for Worldwide Interbank Financial Transactions).

### 2.1.3 Payment by cards

#### 2.1.3.1 Credit Cards

The idea of payment through cards is not new. It first arose in 1915, when a small number of U.S hotels and department stores began to issue what were then referred to as "shopper's plates." It was not until 1947 that Flatbush National Bank issued cards to its local customers. The Diners Club followed this in 1950 and eight years later American Express was born. Since then many card companies have started and failed, but two major card companies made up of large numbers of member banks, have come to dominate business worldwide. These are Visa International and MasterCard. These non-profit associations set standards for the issuing banks that actually issue the credit cards and process transactions. Other third parties (called processing centers or clearing houses) usually handle verification of accounts and balances. Credit card issuing banks act as financial intermediaries, minimizing the risk to transacting parties.

Credit cards offer consumers a line of credit and the ability to make purchases . They are widely accepted as a form of payment; reduce the risk of theft associated with carrying cash, and increase consumer convenience. Credit cards also offer consumers considerable float. With a Credit card, for instance consumers typically need not actually pay for goods purchase until receiving a credit card bill up to thirty days later. Merchant benefit from increased consumer spending resulting from credit card use, but they pay a transaction fee of 3% to 5% of the purchase price to the issuing banks.

In recent years, a great effort has been made to eliminate paper from credit card transactions. This has meant that sales vouchers with the cardholder's signature only come into play when a dispute arises, and most of the information flows electronically. In addition, electronic transactions have much lower operational costs.

A more descriptive diagram of the credit card and its operation will be offered in chapter 7.
More risks are involved in the use of credit cards. According to the BBC news Website (Inside Out, July 7, 2003), [10], in the UK alone credit card fraud cost about 424.6 million pounds (US$771.724 million) in 2003. It is estimated to go over 800 million pounds by 2005, with the increase in the number of credit card users. Banks are becoming increasingly concerned about the escalating costs. In addition, federal regulation ("Fair Credit Billing Act, 1986") [11], places the risks of the transaction (such as credit card fraud, repudiation of the transaction or nonpayment) largely on the merchant and credit card issuing bank. Federal regulations limit cardholder liability to $50 for unauthorized transactions that occur before the card issuer is notified. Once a card is reported stolen, consumers are not liable for any subsequent charges.

We will address the security involved in credit cards in greater detail in Chapter 7.

### *2.1.3.2 Debit cards*

Accounts created by depositing funds into an account and from which funds are paid out or withdrawn as needed are debit cards. They are similar to chequing transfers--which also store funds--but do not involve writing a cheque. Examples include gift certificates, prepaid cards, and smart cards, but rather than providing access to a line of credit, they instead immediately debit a

chequing or other demand-deposit account. However, consumers in the United States have not embraced debit cards to a great extent because they do not offer the protections provided by the regulations ("Fair Credit Billing Act, 1986," [11]) and do not provide any float.

Peer-to-peer (P2P) payment systems such as Paypal are variations on the stored value concept. P2P payments systems do not insist on prepayment, but do require an account with stored value, either a chequing account with funds available or a credit card with an unused credit balance.

Almost all the major banks today issue debit cards. However, like credit cards, they too are prone to fraud. Most debit cards employ a secret Personnel Identification Number (PIN) that authenticates a person during usage. If the fraudsters find out the PIN and can get a copy of the card or its information, they can use the card to withdraw money from the user's account.

#### *2.1.3.3 Charge cards*

These work in a similar way to credit cards, in that payments are set against a special-purpose account. The principal difference is that the entire bill for a charge card must be paid at the end of the billing period. Often, there is no associated spending limit. Some examples include utility, phone, and American Express accounts, all of which accumulate balances usually over a specified period (typically a month) and then are paid in full at the end of the period.

After this brief review of the available payment systems, we should state the difference between electronic banking and electronic money [1]. Electronic banking does not represent a new kind of money, but rather refers to new ways to provide a variety of traditional bank services involving traditional money. Activities such as bill paying and Electronic Funds Transfer (EFT) between accounts over a telephone or computer connection can be considered electronic banking operations. Electronic money refers to the types of stored-value cards or other media that create a new form of money, representing an alternative to government-issued and guaranteed instruments.

In the North American economy, there are many bills to pay. The life-cycle cost of a bill for a business, from the point of issuance to point of payment, is significant. This does not include the

time value of consumers who must open bills, read them, write cheques, address envelopes, apply stamps and then mail payment. The billing market represents an extraordinary opportunity for using the Internet as an electronic billing and payments system that could potentially greatly reduce both the time consumers spend paying bills and the cost of paying them. As consumers increasingly go online, it is reasonable to believe they will want to use the Internet as a means of efficiently paying bills.

### 2.1.4 Electronic Payment System (EPS)

We will start by giving a brief description of the existing electronic payment system. This model is a natural projection of the functionality of traditional payment systems, assuming the participants are represented by electronic devices and that interactions among them will take place over communication channels.

#### 2.1.4.1 A Model for EPS

The following is a model of an electronic payments system (EPS) (see figure 2.1). It shows the essential roles and their business relationships, represented by the transactions executed between them.

The basic set of players involved in each payment consists of:

**Payer** The player who wants to send money to the payee.

**Payee** The player who wants to accept money from the payer.

**Issuer** The payer's bank, which links the electronic payment to a real transfer of money. The issuer may give "electronic money" to the payer to pay with, or may send the money to the payee's acquirer.

**Acquirer** The payee's bank which finally materializes the electronic payment.

In several payment protocols, the "payer" and the "payee" are referred by more specific terms like "customer" and "merchant" or "seller," respectively. Many protocols also use the term "bank" instead of "issuer" and "acquirer."

Certain payment systems might involve more players, such as

- Registration and certification authorities for all players, or

- Trusted third parties that enforce receipts for payments
- Processor

A much-generalized model is shown in the figure 2.1.

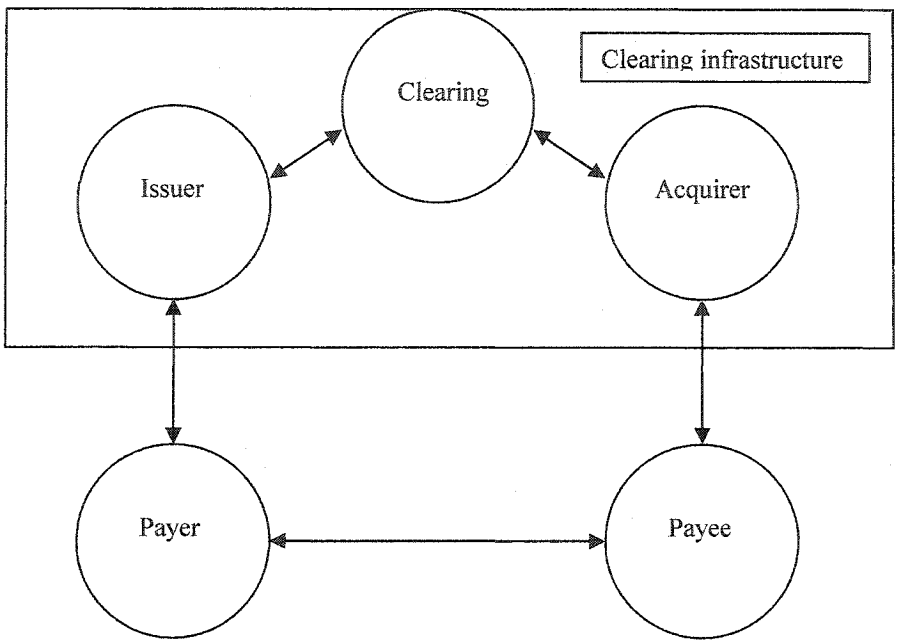



**Figure 2.1 Generalized model of an electronic payment system**

In an on-line payment system, the payer and the payee are connected on-line with a third party (typically issuer or acquirer), whereas in an off-line payment system, the payment is a transaction between two parties only. On-line payments systems are often considered more secure, since the third party can ensure that the payer actually possesses the money he wants to transfer to the payee. In most off-line electronic payments system, double spending of money is prevented by tamper-resistant hardware (smartcards or "electronic wallets"). As a second line of defense, some systems ensure that double spending would be provable, in case it happens (even for systems that offer anonymity otherwise).

The basic transactions of an electronic payment system are withdrawal, collection, payment, and deposit. They are described briefly as follows:

Withdrawal: The withdrawal transaction is executed between the issuer and the payer in order to provide the payer with the electronic payment instruments. This transaction is the direct expression of a contract agreement between the issuer and the payer.

Collection: The goal of the collection transaction is to transfer money from the payer to the issuer in order to update the payer's account according to the underlying contract. The term money is used to refer to coins, bank notes, cheques, and electronic funds transfer instructions from the bank account of the payer to the bank account of the issuer.

Payment: The payment transaction is executed between the payer and the payee. In order to provide the payer with the purchases when requested, the payee asks the payer to produce evidence, using a valid instrument, on the payment claim that specifies the transaction. The payment transaction may or may not be assisted by the issuer (or another third party) to verify the validity of the instrument.

Deposit: During a deposit transaction, the payee forwards all the payment transcripts, the evidences on payment claims, and the corresponding electronic payment instruments, to an acquirer. The evidence can be received by the payee in previous payment transactions, or during an ongoing payment transaction.

The payment mode option of the payment method can be further divided according to the location of the account related to the payer: local account or central account.

### 2.1.4.2 Location of the payer's account

There are two possible options for the location of the payer's account in the EPS:

1. The payer's account is kept within his or her electronic device. In this case, the payer's account is referred to as a local account. The issuer has the option of keeping a shadow (mirror) account of the local account. This allows the issuer to have a better control over the balance update of the local account; also this facility allows the payer to credit her

shadow account with a large initial amount of money, from which she can load her local account several times. Examples of such EPS are, Ecash, Mondex, and PROTON.

2. Only the issuer keeps the payer's account. In this case, the payer's account is referred to as a central account. The payer access the central account using secure mechanism and and handles it himself. Some of the electronic payment systems where the payer has a central account are NetCheque, CheckFree, and Online banking with reader.

# Chapter 3 Electronic Payment Systems

In this thesis, we have chosen to discuss the five most widely used electronic payment systems. The last category, namely, other forms of online banking, consists of the E-payment mechanisms, which are relatively recent. We give the examples of commercial products that are based on them in appendix H. Following electronic payment system will be discussed.

## 3.1. Electronic cash

Electronic cash (e-cash) is a surrogate to paper money. To the users it offers convenience of quick hassle free transaction. Electronic cash is cryptographically crafted to prevent double spending. The encrypted payer's information uniquely identifies the depositor to the bank thus ensuring privacy of the client.

The merchants need to deposit money in the bank to prevent double spending. The banks check for the validity of the money. Banks maintain a large database of issued money serial number. As they receive a request for verification of e-money from the merchant, they look for a match from their database. They also check for the payment information e.g. amount, currency, merchant, payer's information, expiry date, etc. After verification of the e-cash they, send a notice to the merchant with approval or rejection of the e- cash. The merchant sends a copy of notice to the customer and depending on the confirmation starts the process of shipment of goods to the customer.

E-cash does not involve any third party operators. The banks issue, verify and authenticate the cash themselves. No third parties are involved. E-cash systems also use all the existing standards. There is very little cost involved in using e-cash systems. The user needs to install wallet software on his local machine and he can start using it immediately.

E-cash payments systems are traceable. The payment using e-cash system is immediate and in real time. The cash is immediately available to merchant for further use.

E-cash systems have tremendous potential in mobile commerce. However, first the current limitation, such as, slow processing speed of the mobile devices have to be overcome. In addition, the e-cash should be widely available and accepted. E-cash cannot be remotely accessed. The client has to install the wallet software in his local machine. This is not possible remotely.

## 3.2. Electronic Cheque

Electronic cheques work much like paper cheques. The payer writes a cheque to the payee and payee deposits it in his bank. The cheque clears like a paper cheques using settlement and clearing banks. E-cheques is a structured electronic document signed with a digital signature and with the same information as a paper cheque. To make sure that no one changes the information enroute, cryptography is used.

E-cheques offers the same conveniences as paper cheques. Cheques can be written to anyone. E-cheques are secured using SSL protocol. It should be noted that most of the E-cheque systems are web based with the account staying with the bank and customers logging in to their account. The web based systems provide more accountability. Along with giving strong security and accountability, the E-cheque payment systems are versatile. Any changes in the technology can be easily applied. However, like regular cheques, E-cheques do not offer anonymity.

E-cheques systems are gaining greater acceptance. E-cheques do not require any intermediaries. The digital signature can be checked by the merchant who forwards the cheques to his banks for payment. Compared to the paper cheques, the e-cheques costs less to the user. The user has to open account with the bank and the bank provides a secure access to the account. E-cheques are traceable. Unlike paper cheques, the electronic cheques can be checked at any point for authenticity. However, payments made through E-cheques are not immediate. Like paper cheques, the user has to wait for a few days before the cheque goes through payment settlement and clearing bank. Nevertheless, e-cheques have tremendous potential in mobile commerce. Still, issues concerning security on mobile network needs to be resolved. Being web-based, e-cheques can be remotely accessed.

3.3. Credit cards: Credit cards are very different from other electronic payment systems. The payer does not actually pay to the payee at the time of the delivery of goods. The payer settles his bills with the bank at some later point in time.

Credit cards are convenient to the payers, as he does not need to pay money upfront. Users, however, need to make sure that they do not exceed their credit limit. Credit cards when used online employ secure protocols namely, SSL or SET (Appendix E). Privacy is a question while using credit cards SSL v3 protocol. Users should take note of the merchant's privacy policy. Credit card protocols offer strong security to businesses. SSL protocol is in itself very versatile and can be upgraded from time to time. However, SET protocol is not. SSL protocol has been widely deployed and is being used for E-commerce.

Credit cards may require the services of third party operators. Both SET and SSL, protocols have an option of assigning processing of payment card transactions to third party operators. However, in some cases the banks may also choose to perform the role of processors for payments. Credit cards are traceable. The feature of traceability is better in SET protocol than in SSL. Since credit cards do not offer immediate payment, neither merchant nor customer receives any money immediately. SET is resource-intensive protocol and it will be difficult to implement in mobile commerce unless faster mobile processors are developed. SSL has already been implemented in mobile commerce. The credit cards using SSL can be remotely accessed using valid certificates. Most of the browsers support 128-bit encryption so, the users will have no problem using credit card through the web from anywhere.

3.4. Smart cards: Smart cards are relatively new to the e-payment mechanism. Even today, the standards are being resolved. Smart cards offer more security than any other conventional e-payments. Smart cards have computational power within the card itself making it resistant to tampering. The smart card can contain confidential information securely, making it highly desirable for e-commerce.

There are two general types of smart cards "contact" and "contact-less." Smart cards offer tremendous convenience. Usually, they work with a reader, which is connected, to the computer or a network. The payment transaction can be initiated by swiping the card at the reader. The user is asked for a Personal Identification Number (PIN) and the transaction proceeds.

Repudiation is never an issue with a smart card. As the user enters the PIN, the bank assumes that only the authorized user can have both the card and PIN. Most of the smart cards follow a standardized secure protocol during transaction. Some smart cards use SSL protocol while others have their own propriety protocols such as Mondex. Smart card offers privacy and security to businesses. They are versatile. Smart card E-purse upgrades (see appendix E) can be initiated during transaction. Smart cards are gaining popularity. Protocols that were SSL based have already been implemented in the market and newer protocols are still being developed.

Smart cards, which are based on SSL protocols such as American Express Blue, are not free of third party operators. However, some protocols like Mondex do not have any operators and the authorizations are performed by banks themselves. There are costs associated with smart cards such as purchase of readers. Smart cards have tremendous potential in mobile commerce but, they require special attachments such as readers. Many pilot projects have been working around the world to show its utility in the mobile world.

**3.5. Other forms of Online Banking:** The newer forms of online banking namely, banking using a reader, E-mail money transfers and charging to the phone bill, offer all the conveniences of modern day banking. In online banking using a reader the customer can use his bankcard for online purchases. E-mail money transfer can be used through internet. Charging to phone has the advantage by offering accountability.

All three systems offer good security to the consumers. It is the responsibility of the user in the E-mail money transfers to make sure that money goes to the right person. Banks than use the SSL protocol to transfer money to the merchant. Systems requiring charging to the phone bill require users to open an account with bank prior to using the system. These systems also fare very well when it comes to privacy.

The other forms of online banking are more resistant to fraud. They are versatile systems and can be upgraded from time to time. These systems are independent of any third party operators and all the transactions are regulated by banks themselves. They use the existing standard technologies such as SSL. As well, they are easy to implement. Online banking using a reader obviously requires the purchase of a card reader and some user training. Similarly, charging to the phone bill will require the user to purchase a phone modem. Newer forms of online payments fair very well when it comes to traceability. Most of them need the users to have an account prior to start of any transaction.

The money is transferred immediately to the merchant when paid with banking card using a reader. Its takes some time before the transaction proceeds in E-mail money transfers; typically about 24 hours depending on the network and the time taken by the merchant to respond. The users who use the mechanism of charging to phone bill pay their due amount with their phone bill.

The newer form of online payments performs fairly when used for mobile commerce. E-mail money transfer can be easily used using mobile networks. Charging to the phone has already been employed in some parts of world (Japan, NttDoCoMo). The cost of the merchandise is billed along with the users phone bill. However, there are obvious security issues if the phone is stolen or lost. In addition, it becomes expensive as the user pays for both the airtime as well as the merchandise.

Online banking using a reader may not be remotely accessible, as readers may not be available everywhere. E-mail money transfer can be accessed remotely.

# Chapter 4 Results and Analysis

We can say with a considerable degree of accuracy that we have still do not have a satisfactory electronic payment system that meets the needs of both customers and businesses. Credit cards, although quite popular now, have distinct disadvantages: they are expensive to merchants (transaction fees, along with overhead costs: gateway fees, statement fees, tech support fees, etc.) and carry significant security risks. We compare electronic Cheque, digital cash and credit cards in tables 4.1 and smart cards and other forms of online payment in table 1.2. The evaluation criteria have been described in section 1.3. We will rate the payment systems from one to five stars, with *=poor, **=average, ***=good, ****=very good, *****=Excellent.

| **Evaluative Criteria** | **Electronic Cheque** | | | **Digital Cash** | | **Credit Card** | |
|---|---|---|---|---|---|---|---|
| **Customer Proposition** | NetCheque | Check Free | Net Chex | NetCash | Digicash | SET | SSL v3 |
| a. Convenience | *** | **** | **** | ***** | ***** | ***** | ***** |
| b. Security | *** | ***** | *** | **** | ***** | ***** | ***** |
| c. Privacy | **** | ***** | Private | ***** | ***** | ***** | *** |
| **Business Priorities** | | | | | | | |
| a. Security | ***** | ***** | ***** | ***** | **** | ***** | **** |
| b. Versatility | **** | ***** | ***** | *** | *** | *** | ***** |
| c. Acceptance by all Parties | * | **** | **** | * | *** | ** | ***** |
| **Technical Issues** | | | | | | | |
| a. Independence of Operators | ***** | ***** | ***** | ***** | ***** | ***** | * |
| b. Use of Existing Standards | ***** | ***** | *** | ***** | ***** | ***** | ***** |
| **Implementation Issues** | | | | | | | |
| a. Cost Factor | *** | ***** | **** | *** | **** | *** | *** |
| b. Speed to Market | ***** | ***** | ***** | ***** | ***** | *** | ***** |
| **Traceability** | ***** | ***** | ***** | **** | ***** | ***** | *** |
| **Immediate Payment** | * | * | * | ***** | ***** | ** | ** |
| **Applications in Mobile Commerce** | **** | ***** | NA | ***** | * | * | **** |
| **Remote access** | **** | *** | NA | * | * | * | ***** |

**Table 4.1 Comparative evaluation of electronic cheques, digital cash, and credit cards.**

## 4.1 The Customer's Proposition

### 4.1.1 Convenience:

Electronic cheques are more convenient to use than paper cheques. They offer ubiquity and accessibility. However, most E-cheque systems require users to be pre-registered to start using E-cheques. Some E-cheque systems, like NetCheque, require the user to install wallet software on the user's machine; the user must get registered with the ticket issuing authority first. However, other E-cheque software is Web-based, and therefore, can be accessed anywhere (a device with Internet connection). Also, with NetChex and CheckFree people can pay anyone (with valid certificates); however, NetCheque allows you to pay only those people who have registered as NetCheque users and therefore limits its customer base. E-Cheques are also suitable for small value transactions.

Digital Cash tends to offer all the conveniences of regular paper cash. However, most digital cash requires consumers to install special wallet software on their local machines. The software deals with the merchant and bank server and warns the user if any unused portion of digital currency is about to expire soon. In digicash, people have to break cash more often because of the exponential system employed. In NetCash, coins are sent to the bank with an instruction on whom to pay; therefore, it not a direct payment to the merchant. However, it is still very convenient to use for the consumer as he can use them to pay for almost anything. Digital Cash can also be used for small value transactions.

Credit cards are not suitable for micro-transactions as the cost of processing every transaction is very high. However, apart from small value transactions, credit cards are very convenient to use. Users can pay for any merchandise or services based upon their credit limit. It is the only mode of payment which the consumers can use both offline and online universally without having to purchase any extra devices (e.g. readers for smart cards). Both SET and SSL protocols offer consumers equal convenience. In either case, the consumer initiates the payment process and most of the process takes place transparently to the consumer. However, the customer must possess valid certificates before the commencement of the payment process. The browsers today have been programmed to update the latest certificates list and the certificate revocation list

automatically. Credit cards are by far the most developed form of electronic payment and offer their customers more convenience than others.

Smart cards are as convenient as credit cards. Some smart cards function both as stand-alone cards and as an authentication-based card (such as "Blue"). Smart cards aim to offer the flexibility of cash. However, various competing industry standards have limited the scope of smart card usage. With the 1999 launch of CEPS, smart cards are gaining popularity. American Express Blue requires a reader to function fully. Blue can used as both a credit card and an ATM card where acceptable. Multos 4 needs a reader and unlike Blue, cannot be used as a credit card. It offers the unique feature of peer-to-peer payment. However, it needs a reader to operate.

Online banking using a reader offers instant access to funds with ATM card. The customer needs to buy an expensive reader. However, once the reader is installed, the customer can use multiple ATM cards. Also, ATM cards are widely acceptable. With e-mail money transfer, customers can pay anyone who has a bank account with a Certapay acceptable bank. However, not all merchants have accounts with Certapay acceptable banks. This limits its scope. Apart from this, users can be ubiquitous and find it very convenient. Charging to one's phone bill do not offer ubiquity and the user needs to log in to his home PC. Also, the user needs a land phone line to access the system.

### 4.1.2 Security:

Electronic cheques have very effective security features. They are usually safer than ordinary paper cheques, which are checked only at one point (at the issuer's bank). Instead of handwritten signatures, digital cheques are signed with digital signatures. A digital signature is analogous to a fingerprint: it is a unique identifier for a message. A digital signature is the message digest, signed using the sender's private signing key. It should be noted that the message signed with the private signature can be verified only with the public signing key. This is not a means of hiding content from people, but a way to verify the identity of the sender.

A digital signature supports non-repudiation, that it, a recipient of a message must be able to use the digital signature to convince a third party as to the identity of the originator. A digital signature may need to be used as the basis for resolving a dispute between the originator and recipient of a message, such as a cheque or business document.

NetCheque uses symmetric key encryption. To start using the system, all parties must first register. CheckFree uses 128-bit SSL encryption. Also, the system automatically logs out if unused after a time. NetChex uses tools (IdentiChex and VeriChex) to verify the client at the time he is writing the cheque. However, as they are propriety protocols, not much is known about them.

NetCash relies on the establishment of a secure channel between two parties using RSA algorithms or Diffie-Hellman key exchange for network security. The customer bundles the coins with its digital certificate and encrypts them with the merchant's public key. The merchant decrypts the coins, verifies the digital signature of the customer, and send them to the respective currency server (the issuing server) to check for double spending. The NetCash currency contains all the details of the cash encrypted with the issuing server's secret key. Digicash has very strong form of encryption. The coins are encrypted using RSA algorithm and before any transaction is carried out, a hash is compared to ensure the originality of the coins. Ecash systems are further strengthened by using a redundancy-adding function in combination with a one-way hash function.

SET fares very well in terms of security. It makes use of secret-key cryptography, public-key cryptography, digital signatures, message digests, and certificates with trusted third parties. SSL v3 also fares very well in terms of security and, like SET; it uses all the algorithms and cryptography.

Blue employs the benefit of both Java security and SSL v3. Above all, its open source Java development platform enables developers to report any flaws that might exist. Multos 4 uses the Mondex e-purse system and has a propriety security protocol.

Online banking using a reader uses a public key along with certificates issued by a certified authority. E-mail money transfer uses the SSL v3 and therefore is very secure. However, it is the user's responsibility to arrange for a secret question-answer and trust the merchant. Charging to phone bill uses SSL with digital signatures to provide security and is therefore secure.

### 4.1.3 Privacy:

Electronic cheque customers have to rely on banks for a commitment on privacy. Banks collect a variety of information from users at the time of signing of the account. They may use them for understanding our needs, analyze the suitability of banks services, determine our eligibility for their products and services and for the bank's legal and regulatory requirements. NetCheque fares well on privacy. However, it should be noted that the consumer relies on the banks to not take advantage of the information provided by him at signup. The banks adhere to the laws laid out by the government, such as PIPEDA [2] in Canada and HIPPA in U.S. Also, users must check into third party privacy policies when using a service. CheckFree fares well on privacy and only in certain circumstances can user information or details be released. As the CheckFree is Web based and does not need any third party to provide its services, consumer privacy is more secure than with NetCheque. Nothing is said about the NetChex privacy policy on their Web site. They surely must have strong privacy policies as they ask the customer to divulge many personal details such as name, address, city, zip code, e-mail address, home phone numbers, and social insurance numbers at the time of writing the cheques.

If using NetCash, customers have to rely on banks for their privacy. Every time a customer uses NetCash, they have to go through banks, and therefore, banks can build up a database of customer spending habits. However, they are safer than NetCheque because, during the process of issuing coins, customers do not have to inform banks of personal details. Digicash fares well on privacy. The customer wallet software interacts with the merchant's wallet using Internet connections. Therefore, the merchant's as well as the bank's privacy policy should be taken into account.

The privacy policy of the financial institution, the merchants, and the ISP should be carefully read before using credit cards online. Customers have to reveal much personal information during the signup for credit cards and should exercise caution when using them. The privacy of customers is totally protected when using SET for payment. The SET does not divulge any personal or financial information to the merchants. It should be noted that SET protocols start only after the customer has decided which mode of payment to use. It is the customer's responsibility to check on the merchant's Web site for privacy policies. Users have to totally rely on merchants for their privacy when using SSL v3. The merchant can store all the relevant information, such as credit card numbers, the type of card used, name, address (some merchants need these too), and date of purchase.

While using Blue as a credit card, customers have to rely on the merchant if using SSL v3 protocol. When using Blue with a card reader, personal information is stored right on the chip itself and therefore, privacy is guaranteed. Multos 4 uses Mondex e-purse specification and offers very good privacy. It supports person-to-person payment functionality and immediate value transfer. Therefore, no information is stored on the server or any other hardware but on the chip itself.

Customers who do online banking using a reader have to rely on the transaction gateway servers for their privacy. The customer's privacy is totally protected against merchants, who only get information on the transaction approval from the gateway. In e-mail money transfers, customers are assured of their privacy by the banks. Most of the banks have established very strict and restrictive privacy policies. Charging to one's phone bill does not pass any information to the merchants. However, customers have to place their trust on the gateway. The gateway possesses customer information such as phone number and address. Thus, it is vital for the gateway to protect its customers' privacy.

## 4.2 Business Priorities:

### 4.2.1 Security:

Electronic cheques offer good security to businesses. Businesses rely on secure hash algorithms to trust the cheques. The secure hash algorithms are intended to prevent someone from changing the content of any data files. Anyone can verify the signature by decrypting the signature with the corresponding public key, and also computing the hash function of the file. In NetCheque, tickets are used to communicate between merchants and customers so merchants can be sure of the customer's authenticity. CheckFree offers good security to businesses by using SSL protocol and valid certificates. Also, the customers are not anonymous during the process and are therefore accountable. NetChex offers good security to businesses. A user has to enter his e-mail address, home phone number, and social security number along with his name and address. After this, the information is verified through IdentiChex and VeriChex before being conceived.

In electronic cash systems, the businesses base their trust on algorithms. In NetCash systems, the coins are verified first at the currency server; they are verified for double spending and authenticity and then sent to the merchants. Therefore, businesses are assured of the authenticity and validity of coins. In digicash, merchants assume some risk of losing money. The check for double spending is not done at the time of transaction because of the very large digit serial numbers of the currency or tokens. But afterwards, merchants have to deposit the coin with the bank; then a double spending check is performed. The coins are encrypted with the bank's digital signature and allow the signatures to be quickly verified via a plain text version of the serial number that is included with the coin. Also included is information such as value, currency, and expiry date in a file called "keyversion."

The SET protocol offers very good business security. It eliminates the need for the intermediary and all the authorizations are done by banks themselves. The customers need to possess valid certificates even before they can take part in the transaction. In SSL, in some cases where the merchants does not verify the credit numbers in real time,

they may run into trouble if the credit card is stolen. Though credit cards are protected by fraud guarantees [11], there are hassles involved in reclaiming the money.

Smart cards offer good business security. When Blue is reported lost or stolen, the certificates are immediately cancelled and no one can use them. When the card is connected to the reader, no one but the user can access the card. Multos 4, which uses Mondex as an e-purse system, has propriety security mechanisms and has not been publicly announced.

Online banking using a reader provides additional advantages of user authenticity (the user has to swipe the card issued by the bank). The customer uses the public key of the gateway to encrypt his and the merchant's data (merchant's key and certificate) to the gateway. The customer then receives an approval or disapproval message from the gateway with hash, which is forwarded to the merchant. E-mail money transfer offers very secure options for merchants. Customers need to have an account with the bank to e-mail money. Also, the merchant is redirected to a secure site (using SSL) by clicking a link with the e-mail. Charging to one's phone bill offers very good security to businesses. They employ SSL, digital signatures, and a pass phrase for securing the connection. Also, the user is identified by his land line. Therefore, this offers extra security features to the merchants and reduces fraud.

### 4.2.2 Versatility:

Electronic cheques are versatile payment systems. Most of them are server-based and thus, can be upgraded with relative ease. NetCheque can be upgraded by adding more servers (Kerberos) and multiple accounting servers any time. However, on the client side, the user needs to install new software (such updated hash function) to maintain the level of confidence. CheckFree can also be upgraded with relative ease. They are Web-based, and therefore users don't have to prepare the hash of the financial information on the client side. The users just have to login using SSL and they are led securely to the CheckFree Web server. Users, however, need browsers which can update themselves and get the latest certificate revocation list (CRL). NetChex similarly is server based and

therefore, after login the user can access the Web server. Any update or fix can be done at the server's end and remains invisible to the user.

Electronic cash usually employs wallet software on the client side and therefore, remains difficult to upgrade. Also, the wallet software is resource-intensive and might not be suitable for low memory and low processing power systems. In NetCash, the currency is handled by wallet software. It is prepared and then sent to the currency server with instructions on whom to pay. However, the encryption and generation of coins is done at the client's end. Customers have different platforms and hardware, making it difficult to upgrade. Likewise, in digicash, the generation of coins is done by the client's wallet software, and therefore any change in software or any update or fixes might be difficult to perform.

SET is difficult to implement. It is also very slow and resource intensive. It needs users to have custom wallet software, custom merchant software, and special transaction processing software and hardware at the acquirer gateway. The SSL is relatively easy on hardware. Most browsers today come with support for 128-bit encryption. Also, there are patches to older browsers that enable them to work with 128-bit encryption. SSL does not need any custom wallet software installed on the user's PC and the encryption is transparent to the user. This feature makes SSL an attractive option for many different platforms and devices. We have comparatively evaluated both them in thesis (table 7.1). Other researchers have reached to a similar conclusion [12].

Smart cards fare very well when it comes to versatility. They have the advantage of having a microprocessor inside. Having a chip in them, they can be treated as a unit among itself. However, most smart cards need a reader, which are only available for PC and thus cannot be used on mobile phones or PDAs. Smart cards are already being used in a variety of applications. Blue works fairly well when it comes to versatility. It can be used as a credit card and a smart card when used with a reader. It has been developed on the Java platform, and thus various applications can be added to it and existing applications can be modified (such as security). Multos 4, which runs on MULTOS, is

very versatile and different applications can be loaded into the card. To load any application, first, an executable code is formed of MEL byte codes that are output from the compiler/assembler and linker; the data is in the static data structures required by the application. In addition, optional data areas loaded are the MULTOS directory record entry and the file control information record entry. These two optional items are usually specified according to an ISO standard (ISO 7816). Another optional item is the application signature, which ensures the integrity of the executable code and data. Finally, the last item is the key transforming unit, and this allows either all or part of the executable code and/or data areas to be encrypted prior to loading and subsequently decrypted following successful loading. Therefore, any application, such as an electronic payment, can be loaded into Multos 4 with a relevant certificate. The certificates are available at Multos.com.

Online banking with a reader works out well when it comes to versatility. The merchant just sends his data (which includes his certificate) to the customer. The customer then sends the certificate to the gateway where the certificate is verified. The essential part of this system is the card reader. Card readers are only available for PC and therefore cannot be used with other devices such as PDAs or mobile phones. This limits the capability of the system. E-mail money transfer uses SSL to provide security, and therefore both merchant and customer must possess appropriate software (browser) and certificates. Most browsers come with the feature of updating certificates and certificate revocation lists; therefore, e-mail money transfer is very versatile. E-mail can be received on all devices and across many platforms; also, many devices such as mobile phones now support SSL (through proxy). Thus, e-mail money transfer is very versatile. Charging to one's phone bill is only available for users using PCs and who have a modem connected to their phone line. This limits its applications to PCs. In addition, security is provided by the use of SSL and digital certificates, and thus, the certificate revocation list must be updated periodically.

### 4.2.3 Acceptance by all parties:

Electronic cheques payment systems have been widely accepted by all parties. The customers see it as a natural extension of paper cheques and are therefore comfortable using it. However, NetCheque has not been very widely accepted. It has not been released as a commercial product until recently. Every party participating in the NetCheque must have registered with the Kerberos server and obtained ticket before it can participate. It seems impractical when there are so many Internet merchants. CheckFree is widely accepted and it has been in operation since 1999. Last year it earned revenues of $6 billion in payments and about 6 million consumers used it along with about 1 million business. However, to use an online chequing account, users have to be registered first and thus it limits itself. To sign up, users need an e-mail address, their checkbook, driver's license, SIN, and a recent paper bill for each e-Bill the users want to sign up to receive and pay online. NetChex similarly wants users to sign up before they start using the service, and is therefore somewhat limiting. They claim to be completely compatible with current banking infrastructure and do not replace any components of the existing system.

NetCash has not been widely accepted. It has not been released as a commercial product. Digicash is more successful than NetCash when it comes to acceptability. It was the first digital currency to be launched by the banks. However, after three years, it was taken off the market because demand at that time was not high. It was the dawn of the Internet age and e-commerce was just picking up.

SET has not been widely accepted, especially by merchants. The customer largely remains anonymous to the merchant and they rely on the bank's communication for the approval or rejection of each transaction. Also, SET is the most complicated protocol ever designed and its interoperability over different implementation is a problem. SSL, on the other hand, was released in 1996, and since then has become a *de facto* protocol for Internet payment transactions, when it involved a card. It is being widely used and it's being implemented in the field of wireless data networks.

Smart cards are widely being accepted in the market. Their demand is increasing every year and according to MasterCard, smart card activity has been particularly high in the Asia/Pacific region where the number of EMV smart cards today stands at 14.5 million. Blue has been widely accepted. It offered the industry's first smart card application that can be downloaded from the Internet. Its features included online security, loyalty applications, and secure point-of-sale payments. In addition to smart chip features, Blue carries no annual fee, a low fixed interest rate, and a fee-free rewards program. Multos 4 is also gaining popularity, although it cannot be used as a credit card but rather as a charge card. The card is typically loaded at the time of issue and can be used at retail stores at point-of-sale terminals as well as on the Internet with a reader. However, it can only be used with a PC with a reader, and no reader has been made for mobile devices.

Online banking using a reader does not have many takers. One of the reasons is the requirement of purchasing a reader. Also, the system cannot be made available to other devices, such as mobile phones and PDAs. Also, there is a question of security and trust on the transaction gateway, where the merchant certificate is verified along with the consumer's information. E-mail money transfer is being offered by banks and thus it is widely accepted by all the parties. It employs the same security mechanism as the banks. Charging to one's phone bill is not widely popular.

## 4.3 Technical Issues:

### 4.3.1 Independence of Operators:

Electronic cheques do not involve any operators. The bank sets up the rules governing them, issues them, and operates them. NetCheque does not involve any operators. The customer prepares the hash of the cheques and sends it to the recipient, the recipient submits the details to his or her bank, where it follows normal ACH network. No third party gets involved at any stage. CheckFree acts as an online bank and it's the banks themselves that take on the responsibility of mailing off the cheques. No third party gets involved. Similarly, in NetChex, no third party gets involved.

In NetCash and digicash, no third party gets involved. The software wallet installed at the user's local machine generates the coins or tokens. The wallet software also takes care of the transfer and validation of coins. The merchants have to deposit the coins at the bank immediately, and it's only the bank, which can check for double spending. Thus, no third party gets involved.

Merchants accepting credit cards as a form of payment sometimes outsource the payment processing to a third party. It should be noted that in SET protocol, the third party does not sees the credit card numbers. They are encrypted using the payment gateway public key. In SSL the third party can see the credit card numbers as they are encrypted using the third party public key.

Smart card similarly needs a third party to cover a wide area. Blue when being used as a credit card may depend on third party operators. However, its added security makes sure that no one but the bank's payment gateway sees the consumer's credit card numbers. Multos 4 using Mondex e-purse specification does not involve any third party.

Online banking using a reader does not involve any third party. They themselves act as a payment gateway and the authenticity of the merchants and send all the information to the banks for approval. E-mail money transfer is a service owned and operated by the banks and thus does not involve any third party. Charging to one's phone bill does not involve any third party.

**4.3.2 Use of Existing standards**:

NetCheque uses existing and trusted technologies. It is based on Kerberos server authentication and uses secure hash algorithms to prevent someone from changing the content. Both have been well tested. CheckFree uses SSL technology to encrypt the link. SSL has become a *de facto* standard when it comes to securing data online, and therefore, well trusted. CheckFree also guarantees bill payment. The bills that cannot be paid electronically are paid by cheque. NetChex uses proprietary protocols to provide security (IdentiChex and VeriChex).

NetCash establishes a secure channel between users first by using an RSA algorithm or a Diffe-Hellman key exchange protocol. Once the secure channel is established, the sender sends his coins to the receiver along with his digital signatures and certificates. Ecash is also based on tried and tested algorithms (such as, RSA, SHA). RSA algorithms have been the most widely used algorithm and are thus well tested and tried.

SET uses certificate management to authenticate different parties. It also uses various tried and tested algorithms. Similarly, SSL uses certificates to authenticate parties and thus, append to the standards.

Smart cards are relatively new to payments. Standards have been set on the hardware of the card (ISO 7816), and in 1999, a company formed CEPSCO, LLC, to promote common electronic purse specification. According to the CEPS Web site, currently, organizations from over 30 countries, representing more than 90% of the world's electronic purse cards, have agreed to implement CEPS. Blue uses Java as well as SSL to provide security. It is based on the ISO 7816 standard, runs on Java-based operating systems, and supports CEPS, Proton's e-purse. Multos 4 is also based on the ISO 7816 standard; however, it supports Multos operating systems and Mondex e-purse. It does not support CEPS.

There has been no standard set up for online banking using a reader. The transaction gateway uses the merchant's certificates and digital signatures to authenticate the merchant. It is not known how the customer sends all the details of transactions to the transaction gateway, as the protocol remains proprietary. E-mail money transfer uses all the existing protocols. E-mails are based on the standard as mentioned by Internet engineering task force. Then the payee is asked to click a link, which uses SSL security and leads him to the bank server. Charging to one's phone bill uses SSL, along with digital signatures, to ensure the security.

## 4.4 Implementation Issues:

### 4.4.1 Cost Factor:

Electronic cheques involve very low cost in implementation. At the time of sign up, the user is given a floppy or a compact disc or downloads the software wallet. After installation, the system is ready for use. Similarly, the cost to the merchant is very small. The system relies on Kerberos server authentication technology and a service fee may be levied on users to maintain the Kerberos server. At this time, it's hard to say who will pay the fee, as no commercial implementation has been conceived. Many financial institutions offer CheckFree free, though; some may charge a small monthly fee. The users have to open a bank account with the CheckFree first. The transaction fee for processing online cheques in NetChex is very small. However, there might be a small fee levied on the merchants too.

NetCash involves an extra cost to the banks that have to maintain a huge database to store the serial numbers of the used coins. Also, NetCash users need to have an appropriate certificate from the currency server that generated the coins. These involve extra costs. Ecash users have to install wallet software and, as in NetCash, the banks have to maintain a database of spent coins.

SET is a robust, complex, and resource-intensive protocol. It involves quite a price to the merchant along with some risks. However, the consumers do not have to pay any fee for using the system. Similarly, SSL involves a hefty price tag on the merchant's part. Some merchants choose to outsource the transaction processing to a third party processor. The third party fees include set-up fees, per transaction fees, and refund fees.

Smart cards always involve an extra cost to purchase a reader on the consumer as well as on the merchant side. On the merchant side, merchants have to maintain a system that supports most of the e-purses available in the market, therefore involving extra costs. Blue, when used as a credit card, offers the same advantages and disadvantages as other credit cards.

Online banking using a reader involves the extra cost for the consumer of purchasing a reader. Merchants need to have an account with the Ecash networks and with the bank in order to operate. E-mail money transfer offers tremendous cost advantages. The payer has to pay hefty transaction fees per transaction, but the payee does not pay anything. Both payer and payee need to have accounts with the bank. Charging to one's phone bill compels the user to have a land line and a modem in his computer connected to his phone. Merchants need to have an account with eCharge to accept the transaction and thus maintain a network with the eCharge gateway.

**4.4.2 Speed to Market:**

NetCheque would be very fast in implementation. Software wallets make the process easy to understand. The user fills out the cheque exactly as he would a paper cheque and makes the payment. It's the software wallet that makes the call for the ticket and sends the cheque and its hash to the bank. CheckFree and NetChex have already been implemented and have been very successful.

NetCash is quite similar to cash and thus should have no problems in being implemented in the market. All the encryption and secure transfer parts would be taken care by the software wallet. Similarly, digicash has been successfully implemented.

SET may take a while before being completely implemented in the market. SET is very robust and complex. It will take a while before one is completely satisfied using the system. Also, it involves many parties and thus needs to have a reliable connection between them. SSL is already in use and has been quite successful in implementation.

Smart cards, being very new, will take a while before they are completely absorbed into the market. Blue has the advantage of being used as a credit card, and therefore it was easily absorbed. It also provided much needed additional security. Multos 4, on the other hand, needs to educate the people about the advantages of having a smart card. It will also need to set up networks and protocols as required.

Online banking using a reader needs to convince the users to buy a reader. Some effort will also be needed to build up a relation with the merchants. E-mail money transfer has already been implemented and has been quite successful so far. Charging to one's phone bill provider, "eCharge," will need to convince people of the advantages of the system, and convince them to purchase a modem. Besides, they would also need to build up a relationship with the merchants.

## 4.5 Traceability:

Electronic cheques are traceable. The users have to be registered with the bank before they can start writing cheques. Similarly, CheckFree and NetChex are traceable.

A NetCash user remains anonymous. However, banks may trace users if they choose to. Digicash similarly offers anonymity to the buyer (by the use of blinded signatures) and are not traceable. The merchants are traceable as they have to return the money as soon as they get it to check for double spending.

In SET, transactions are traceable. But this can only be performed by the banks as they have all the information pertaining to the transaction. Neither the merchants nor the third parties are privileged to any of the transaction details. In SSL, the merchant can see the client's information if he chooses to do so.

In Blue, banks can trace the cardholder. However, a Multos 4 user becomes untraceable. Once the card is sold with prepaid cash, the users can use it anywhere. Two users can even exchange currency between them.

Users of online banking using a reader are traceable. They need to open an account with the bank before they can start using the system. Customers can be traced if they choose to use e-mail money transfer. An account has to be opened first before using e-mail money transfer. Similarly, users who charge to their phone bill need to have an account with the bank before they can start using the system.

## 4.6 Immediate Payment:

Net cheques has not been implemented and thus, it cannot be said how much time it takes before payment is delivered. Ideally, it should be within 3 days from the date of issue. The payee receives the cheques electronically and deposits it in his account. The bank then takes cheques and processes it with normal automated clearing house regulations. Similarly, NetChex and CheckFree take almost 4 to 5 business days. The time taken by the automated clearing house is typically around 3 to 4 business days. Also, it may take more by CheckFree if the cheques have to be printed and mailed out.

In NetCash and digicash, the payment is immediate. However, it depends on the time taken by the banks to match the serial numbers from the spent currency serial numbers list.

The payments are not immediate when using a credit card. The consumers build up the credit for a period of time (typically a month) before they pay their balance. The merchants have to wait for approximately 48 hours before they get their due amount. However, some merchants start the shipment of goods immediately after the approval; or they can wait for the cash to be present in their account before they ship.

In Blue, the payment is not immediate. Customers have to wait for a month before the bill comes. Merchants have to wait for approximately 48 hours. However, in Multos 4, the payment is immediate and is immediately available for use.

In online banking using a reader, the funds are available immediately. The process works much like Interac. The merchants can access the funds. In e-mail money transfer, the funds are immediately delivered to the payee account. However, it is the network that decides the speed of the e-mail delivery. Users who charge to their phone bill have to wait a whole month before they receive the bill (along with the regular phone bill).

## 4.7 Applications in mobile Commerce:

NetCheque could be applied in mobile commerce. As it uses a Kerberos model (symmetric key), it requires each user to generate tickets to sign their cheques. These tickets may expire frequently, which would require a more robust, on-line environment, which does not exist so far. CheckFree employs SSL encryption, which is now possible using WAP 2, and therefore it can be easily employed using a WAP 2 connection. NetChex uses propriety protocols to provide security and thus, nothing much can be said about their applicability in mobile commerce.

NetCash uses Kerberos model for security and thus demands lots of processing power, which might be difficult of small processors of the mobile devices of today. Digicash employ public keys, digital signatures, certificates and other algorithms. It might be very slow because of limited mobile processor speed and memory.

SET is very resource-intensive and requires a robust channel to communicate between parties, and therefore might not be suitable for mobile commerce. SSL has been modified into WTLS before being employed in wireless networks. It has been in use for a while now.

Blue can be used for mobile commerce only like a credit card employing WTLS. However, there is no reader available for mobile phones, and thus, we cannot take full advantage of the smart chip within the card. Multos 4 cards have a good opportunity in the field of mobile commerce. Their unique peer-to-peer payment feature makes it an attractive choice for mobile commerce. There are several pilot projects working on the implementation of Multos4 on mobile commerce [13].

Online banking using a reader does not support mobile commerce now. It might be possible with some special reader integrated with the mobile phone. E-mail money transfer has good employment in mobile commerce. Most mobile phones today allow users to send and receive e-mails and perform online banking. They also allow SSL connection, and thus, users can send and receive money from their mobile phones.

However, it should be noted that the bank should have the Web site in WTML format (for WAP network) to be accessed by cell phones. Charging to one's phone has already been employed in some parts of world (Japan, NttDoCoMo). Users buy things from the cell phone and they are billed along with their phone bill. However, obvious challenges occur if the phone is stolen or lost. Also, it becomes expensive as the user pays for both airtime as well as the merchandise.

## 4.8 Remote access:

NetCheque can be accessed from any location. The trust is obtained by the Kerberos server. The user calls for the ticket and upon creating a successful secure link between him and the server, he proceeds. Most devices support symmetric key encryption, however, the processor and memory limits the size of the key. CheckFree employs SSL encryption technology and thus, the user can access it from anywhere, which supports SSL. Some old browsers (browsers prior to IE 5.02 or Netscape 4.76) that do not support 128-bit encryption won't be able to access CheckFree. NetChex employs propriety security protocols and thus, not much can be said about them.

NetCash and digicash are dependent on public/private key exchange pairs. They need resource-intensive processors. Also, they need wallet software installed on the local machine before they can be used, which might not be possible in every situation.

SET is a very robust and resource-intensive protocol and cannot be accessed from everywhere. It's currently having problems with implementation on cross-platforms. SSL has been implemented very successfully. It has become the *de facto* standard for online security.

Blue can be easily accessed as a credit card from anywhere; however, to take full advantage of its features, a reader must be installed. The user may purchase a reader and keep it with him. However, it should be noted that the reader needs a serial port, which might not be available everywhere (e.g. with Macintosh systems or Sun systems). Multos 4 needs an appropriate reader to transfer cash.

Online banking using a reader is also dependent on a reader that might not be available everywhere. E-mail money transfer can be accessed anywhere (wherever SSL is supported). It is totally Web-based and needs users to have an account with the bank to send or receive money. Charging to one's phone bill does not work from everywhere. It needs a land line and a connection to the modem in the computer. Also, the user cannot use someone else's phone.

| **Evaluative Criteria** | **Smart Cards** | | **Other forms of online payment** | | |
|---|---|---|---|---|---|
| **Customer Proposition** | Blue | Multos 4 | Banking using Reader | E-Mail Money | Charging to one's phone Bill |
| a. Convenience | ***** | **** | ***** | ***** | *** |
| b. Security | ***** | Propriety | ***** | ***** | ***** |
| c. Privacy | ***** | ***** | ***** | ***** | ***** |
| **Business Priorities** | | | | | |
| a. Security | ***** | Propriety | **** | ***** | ***** |
| b. Versatility | **** | **** | **** | ***** | *** |
| c. Acceptance by all Parties | ***** | *** | *** | ***** | **** |
| **Technical Issues** | | | | | |
| a. Independence of Operators | *** | ***** | ***** | ***** | ***** |
| b. Use of Existing Standards | ***** | *** | ***** | ***** | ***** |
| **Implementation Issues** | | | | | |
| a. Cost Factor | *** | *** | **** | **** | *** |
| b. Speed to Market | ***** | *** | **** | ***** | ** |
| **Traceability** | ***** | * | ***** | ***** | ***** |
| **Immediate Payment** | ** | ***** | ***** | ***** | ** |
| **Applications in Mobile Commerce** | **** | **** | ** | ***** | **** |
| **Remote access** | *** | *** | *** | ***** | * |

**Table 4.2 Comparative evaluation of smart cards and other forms of online payments.**

# Chapter 5 Summary and Conclusions

Use of electronic commerce is growing at an increasing pace every year. There is a definite need for viable and reliable electronic payment systems that cater to the demands of present day online business transactions. In this thesis, various online payment mechanisms were analyzed, and their strength and weakness discussed. Here, we will summarize our findings and conclude with recommendations for improved mechanisms that meets the needs of consumers and business today.

Almost all the payment systems are dependent on certificate management and yet there are issues with certificate management [14 & 15]. Special care needs to be taken on the size of selected keys. Since public key certificates have relatively long lifetime, the information they contain can become invalid during their lifetime with high probability. Therefore, a set procedures to check certificate revocation information should be used.

Electronic cash uses robust and resource intensive protocols, which may not be suitable for devices with low computational power (hand-held devices). In addition, all the electronic coins or currencies have to be sent to the bank immediately for verification to prevent double spending and fraud. Thus, electronic cash needs a sound protocol which is secure enough to prevent double spending and fraud and yet simple to use.

Electronic cheques are more accountable than other payment systems. Also, most e-cheques do not require any software installation. Therefore, electronic cheques should be targeted mostly to business-to-consumer or business-to-business dealings, where accountability rather than anonymity, is the major concern.

Credit cards are an attractive payment option for both online and offline transactions. However, drastic steps are needed to reduce fraud. The operating cost of credit cards needs to be lowered to accommodate micro payments. Two competing protocols (SET and SSL) enable the use of credit cards on Internet. The industry needs to select on one protocol and use it consistently. In

addition, the businesses need to address the consumer's privacy and anonymity issues when using credit cards are used.

In our opinion smart cards are by far the best bet for future currency. In addition to providing strong security, they can also be used for micro payments and mobile commerce. However, it should be noted that smart cards need card readers to take full advantage of their capabilities. In addition, a smart cards, like credit cards, can be used in online as well as offline or retail transactions. We need a simple yet secure protocol that generalizes the use of smart cards.

Newer online payments mechanisms being developed should offer distinct advantage over the ones that are already in use. In addition, they need to address the issues of certificate management where applicable. They should be deployable in mobile devices and should offer ubiquity to consumers. The new forms for online payments should provide all the needed devices (such as reader) free to the consumer's. In addition, they should provide consumers with guarantees against fraud.

It is clear that a satisfactory electronic payment system that caters to the needs of both customers and businesses has not yet been developed. Credit cards, although popular now, have distinct disadvantages. It is apparent that there is scope of development of new electronic payment systems along with improvement in existing ones.

# Appendix A

# Encryption and Cryptography

Before we move ahead and describe the various electronic payment systems in the market today, we should understand the technology behind the security features as implemented by these systems.

Anyone who wants to accept a pile of bits that claims to be worth something will want some way to verify the bits. Any digital monetary system requires the equivalent signature that proves that someone is going to stand behind the value that is encoded in the pile of bits. On the face of it, it seems to be an impossible proposition. Bits can easily be changed in such a way that no one can find out.

The solution lies in mathematics. There are complicated mathematical functions known as digital signatures that can simulate every feature of manual signatures. These digital signatures can only be produced by someone who knows the secret keys, yet can be checked by anyone. The mathematical foundations of these signatures seem to be strong enough to prevent anyone from forging the signature without the secret key.

Digital signatures are often created from several different algorithms or equations. We will explain the most widely used algorithms used in the market today and also some other encryptions algorithms that are useful in constructing digital cash systems and facilitating electronic payments.

## A.1 Private-Key Encryption

These encryption systems scramble data so it can only be understood by someone who possesses a single, secret, or private key. This key is a large number and the same key must be used to lock and unlock the data. Some of the most common private-key systems are the U.S. government's

Data Encryption Standard (DES); triple-DES, which repeats DES three times for good measure; RC-4, a propriety algorithm from RSA Data Security; and IDEA.

Private-key encryption is not widely used in electronic payment systems. According to the "Encryption and Security Tutorial" by Peter Gutmann [16], a DES with a key size of 56 bits takes about $2^{55}$ attempts with brute force, $2^{47}$ attempts with differential cryptanalysis, and $2^{43}$ attempts with linear cryptanalysis. DES can be broken using field-programmable gate array (FPGA) and application-specific integrated circuits (ASIC).

## A.2 Public-Key encryption

These algorithms scramble data with two different keys. One is used to encrypt the data and the other is used to decrypt the data. Interestingly, the one that is used to encrypt the data cannot be used to decrypt the data. One of the best features of this algorithm is that it allows people to communicate without meeting to set up a secret key. Each of the members publishes one of their two keys (public key) and keeps the other one secret (private key). Each then uses the public key of the recipient to encrypt the message. Only the holder of the corresponding private key can decode the message.

The most popular form of public-key encryption today is RSA system developed by Ron Rivest, Adi Shamir, and Len Adleman [17]. The trio developed the system when all three were at the Massachusetts Institute of Technology in 1978, and the university patented the system in their names.

The RSA algorithm [18] is based on the fact that it is difficult to factor very large numbers. The basic algorithm works as follows;

1. Two very large distinct primes say, p and q are chosen;
2. Compute the product (modulus) say, n = p*q;
3. Compute the Euler's totient function say Q(n)= (p-1)*(q-1);
4. Randomly chose an encryption key e, such that e and Q(n) are relatively prime;

5. Finally, calculate the decryption key d, the multiplicative inverse of e mod Q (n), i.e., $d = e^{-1} \bmod (p-1)*(q-1)$;

Note that d and e are also relatively prime. The numbers e and n is the public key. The number d is the secret key. The two prime's p and q are never needed again. They are discarded and never revealed. To encrypt the message M, we first break the message into series of blocks and represent each block as an integer. The block size is chosen to ensure that this integer will be smaller than n.
i.e., $C = M^e \bmod n$;

To decrypt the resulting cipher text C, we raise to another power d modulo n,
i.e., $M = C^d \bmod n$;

Thus with RSA, each owner of a key pair holds *d* secret, and issues *e* and *n* as his public key. The security of RSA depends on the problem of factoring large numbers. Currently, 512-bit numbers are used as moduli, a product of two 256-bit primes ($2^{256}$ is about 80 decimal digits). It takes at least a year for a high-end home computer using the fastest available algorithm to break RSA. However, today in applications where key compromise would have very serious consequences or where the security must remain valid for many years into the future, key lengths of 2,048-bits is typically used.

Note that performing exponentiation with numbers of this size is expensive in terms of computing resources. A typical software implementation of a symmetric encryption algorithm (e.g., DES) would be around 100 times faster than RSA, while hardware implementations would be between 1,000 to 10,000 times as fast. Quite often, private keys are actually encrypted by public keys and distributed online. The result being that the encryptions are actually performed by private keys and thus, faster to encrypt and decrypt. At the same time they offer the advantages of being distributed securely. For an example, a typical secure email client would use the private keys to encrypt the mail and distribute the encrypted private keys using public keys to ensure only the person with the correct key can decrypt the private key out.

One of the major problems is providing people with a way to be sure that a published key is authentic. This problem can lead to eavesdropping and compromised traffic. This can be illustrated by the following example. Imagine that we have created a secret key *e1* and published key *d1*. An interloper with access to the public directory of keys creates key *e2* and substitute's *d2* for my key. Someone sends me a message, mistakenly encrypting it with d2, which allows the attacker to decrypt it with e2. The attacker can read the message, modify it if desired and then re-encrypt it with d1 before passing it on to me. I would not guess that there was anything wrong.

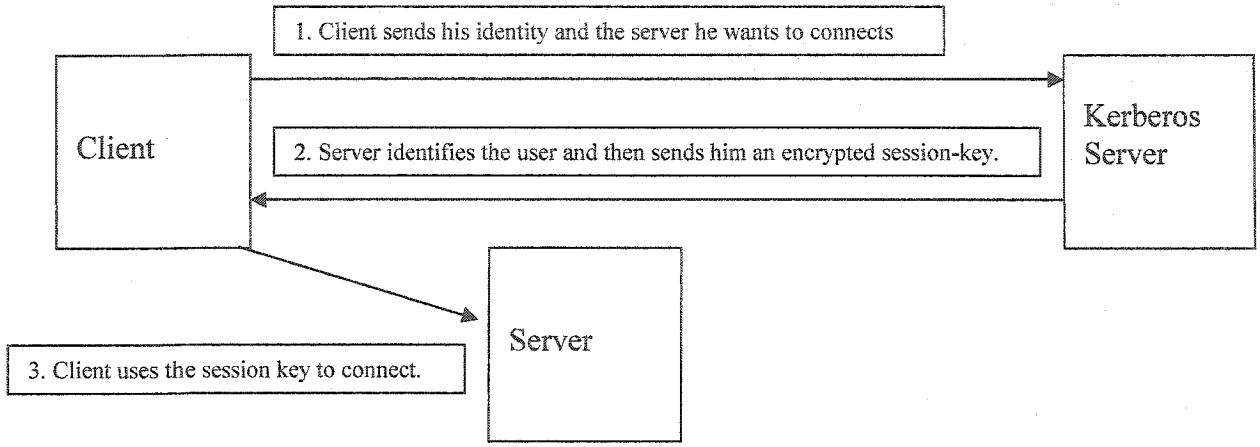
There are two major approaches to solve this problem. One involves a central authority like the government, bank, or a private company set up to be a trusted party. It uses a digital signature, which will be explained in detail in the following page. The other one uses PGP (Pretty Good Privacy) software first developed by Phil Zimmerman. The software uses a "Web of trust" to bind all the public keys. I might receive a public key from "a" and it comes with signatures of "b," "c," "d" attesting its authenticity. I don't know "a," but I know "b." Knowing this, I can verify the signature of "b" and this proves that the public key of "a" is authentic.

Public key systems are the most widely used systems for electronic payment. They are used to encrypt the message with the receiver's public key to achieve confidentiality, or encrypting a message with the sender's private key to achieve message authentication.

## A.3 Kerberos

Kerberos [19] is a complete authentication system. It is based on symmetric cryptosystems. Kerberos was designed as a part of Project Athena at the Massachusetts Institute of Technology (MIT). Kerberos can be used to authenticate the identity of the client to the servers and vice-versa.

The process starts when the client requests a ticket from the Kerberos server. The user sends his identity and the name of the server he wants t o connect. The Kerberos server verifies the client's identity and generates a new random key, also known as the session key (it will be used only for that session). It encrypts the session key with the secret key of the client (the server stores the keys of each principal on the network).




It then creates a ticket for the end-server that includes the session key. The contents of the ticket are encrypted using the shared key of the end-server that the Kerberos server obtains from its secure database. The Kerberos server sends the ticket, along with an encrypted copy of the session key, back to the client. Once the client has received the response, the client uses his or her key to decrypt it. It is this exchange between a client and a target server that authenticates a client to a server and optionally the server to the client.

Kerberos includes procedures for use across multiple domains, called realms, which employ independent authentication servers, possibly under the control of separate organizations. A comprehensive administrative protocol is also defined.

The main attraction of Kerberos is that it provides a good level of protection, and uses relatively inexpensive technology. Disadvantages include the need for trusted (physically secure) online servers; also, there are difficulties in scaling to arbitrarily large populations. Thus, as the number of people using electronic payment grows there is obviously a problem of scalability.

## A.4 Hash Functions

Most of the time a check on message integrity is all that is required. Hash functions check the integrity of the message, and thus do not waste time and resources in encryption. In many cases, the businesses would not be concerned with the eavesdropping on the message but they would certainly be concerned if the message is altered on the way.

The main purpose of the hash algorithm is to come up with relatively short numbers that could be used as surrogates for large files. These are quite useful because we can use a signature algorithm to sign the surrogate instead of the whole file, and thus saving time. A hash function serves the dual purpose of providing a random number for two people separated by time or space in an indisputable way. An inference for the need of hash algorithms can be drawn from the non-cryptographically secure hash function known as the "checksum." This is widely used in many file transfer protocols to determine whether an error occurred during transit. Someone sending a file would add up all of the bytes of data and append this to the end of the file. The person at the other end would do the same thing. Since there are 8 bits in the checksum byte, there are 256 possible values and a 1/256 chance that a random error will leave the checksum unchanged.

Two very important properties that hash functions should have are being (1) difficult to invert and (2) being collision free. The first one means that attempts to produce a message that would yield a given hash should be completely infeasible. Resistant to collision means that the probability of finding two messages with the same hash should be very low.

Two well-know hash functions that have found a place in payment protocols are MD5 [20] and Secure Hash Algorithm (SHA) [21]. The MD5 algorithm is one of a series (including MD2 and MD4) of message digest algorithms developed by Ron Rivest.

## A.5 Digital Signature

To ensure that the message digest created by the sender is not tampered with en route to the recipient, a digital signature is created. A digital signature is analogous to a fingerprint--it is a unique identifier for a message. A digital signature is the message digest signed using the sender's private signing key. It should be noted that the message signed with the private signature could be verified only with the public signing key. This is not a means of hiding content from people, but a way to verify the identity of the sender.

A digital signature supports non-repudiation, that is, the recipient of a message must be able to use the digital signature to convince a third party as to the identity of the originator. A digital

signature may need to be used as the basis for resolving a dispute between the originator and recipient of a message, such as a cheque or business document. The party with the most gain by falsifying the message will very likely be the recipient. Hence, the recipient must not be able to generate a digital signature which is indistinguishable from one generated by the originator.
Some of the commonly used algorithms are R.S.A Digital Signatures and Digital Signature Algorithm (DSA).

DSA is based on a different mathematical problem than that of RSA--the discrete logarithm problem, or the difficulty of inverting a mathematical exponentiation operation in a finite field. One interesting difference between DSA and RSA is that an implementation of DSA does not provide any capability to encrypt data for confidentiality purposes. While this may appear to be a deficiency, it can also be a benefit, because it can be more difficult to obtain export approval for equipment capable of encryption. Another characteristic of DSA is that its verification process is much more processing-resource-intensive than that of RSA.

Digital signatures are used in almost every form of electronic payment system. It identifies the originator of the message and thus builds up trust in the whole process. The sender first finds out the hash of the message, and then encrypts it with the sender's private key. Now the signature is appended to the message.

## A.6 Discrete Log Signature

These signatures are the basis of digital cash systems as described below. This algorithm takes its strength from the fact that it is very difficult to compute $g^a \bmod p$ when p is very large prime number, g is generator ($1<g<p$), and $a$ is an integer.

The following steps will describe the working principle behind the discrete log algorithm:

1. First the documents are run through a hash algorithm, and the output is, say, "m." It can be signed by computing $m^X \bmod p$ where x is a secret key and p is a large prime number. Then the values $m^X \bmod p$, g, p and $g^X \bmod p$ are published.

2. To verify the signature, first you select a random number "w" and calculate $g^w \bmod p$, keeping "w" secret. You ask for the person you want to verify your signature for a random number, say "c." You send him the value $r = c*x + w$
3. The person computes $g^r \bmod p$ and compares it with $(g^X)^c * (g^w) \bmod p$. They should be same.

The system can be made non-interactive and more practical by using a cryptographically secure hash function. A hash function of many of the principal values serves the same purpose as the random number "c." The basic principles standing behind a secure hash practically guarantee that no one will be able to control the value of the "c."

1. Instead of waiting for someone to verify the signature and sending the value of "c," we select the value of "c" by using a secure hash algorithm to hash up the values of $m^w \bmod p$, $m^X \bmod p$ and $g^w \bmod p$ arranged in the standard format and attached to the message itself. It is important to note that we cannot control the outcome of this step.
2. Now, we attach four numbers r, $m^w \bmod p$, $m^X \bmod p$, and $g^w \bmod p$ as the signature. The value of r comes from $r = c*x + w$.
3. Any challenger can check this signature by computing "c" by hashing the four numbers m, $m^w \bmod p$, $m^X \bmod p$ and $g^w \bmod p$ and then computing $(g^X)^c * (g^w) \bmod p$.

A prearranged and practically non-negotiable process like the hash functions can act as a good surrogate. Normally, secure hash algorithm (SHA) is used these days.

## A.7 Blinded Digital Signature

Blinded signatures are widely used where we don't want the signer to know the content he is signing. Blinded signatures were invented by David Chaum and are patented in his name [22]. Mathematically, the blind signatures work as follows:

1. To sign a message "M"; the sender chooses a random number say "k," where k is between 1 and "n," the prime moduli (based on RSA algorithm).

2. The sender then computes $M*k^e$ mod n and sends this number to the signer.
3. The signer then signs the message with its private key say "d," $(M*k^e)^d$ mod n and sends it back to the sender.
4. The sender then retrieves the original message by unbinding the random number that he had included in the beginning i.e., $(M*k^e)^d$ mod n / k.

However, it is worth mentioning that the blind signature algorithms are modified to some extent before being used, because once the signature is signed the document becomes irrefutable.

## A.8 Dual Signature

Dual signatures are used to link an identity with the content of a particular message. In order to verify the message, the recipient must also be able to access the message content. The dual signatures provides a link between a message and an identity without the need to be able to see the message contents completely.

The construction is simple: first, the two messages are hashed, and form individual digests; then the digests are hashed to form a single hash, which is signed by the sender's private key. The application of dual signature can be shown in the following example; suppose a merchant wants to send his client an offer to purchase a piece of property and an authorization to his bank to transfer the money if the client accepts the offer; but the merchant does not want the bank to the terms of the offer nor does he wants client to see his account information. Further, merchant wants to link the offer to the transfer so that the money is only transferred if the client accepts his offer. All this can be accomplished by digitally signing both the messages with a single signature operation.

## A.9 Nonces

To protect against replay attacks--attacks, which focus on sending the same message repeatedly rather than on breaking an algorithm--Nonces are used.

A good example of reply attacks would be in case of an hacker who has an access to one's computer notices the same set of messages sent while conducting a financial transaction over a period over the Internet. He replays the messages and impersonates the customers.

A simple nonce would be an ever-increasing integer, where the party contacted could keep track of the numbers that had been used to date. However, in practice, Nonces are a function of time, together with a randomly generated quantity.

## A.10 Public-Private Key-Pair Management and Certificates

Since its inception, public-key encryption has been hugely successful. Like many successful systems, it is not without its weaknesses. One main problem of the public key is key-pair management. There are always questions about the originality, distribution, storage and revocation of the keys.

The public key pair is used as follows: after generating a pair of keys, the user keeps one component secret and publishes the other component. If the sender wants to send an encrypted message, he or she looks up the public key of the receiver and uses it to encrypt the message. The receiver then uses his secret component of the key to decrypt it. Thus, anyone who has access to receiver's public key can send him an encrypted message, but no one except the receiver can decrypt it.

A certifying authority (CA) solves this problem. The Certification authority guarantees the authenticity of the keys and hence the individual and the parties themselves. The certificates are obtained as follows:

A. The sender generates a key pair and signs the public key and identification information with the private key. This accomplishes two functions:
    - Proving that the sender holds the private key corresponding to the public key.

- Protecting the public key and ID (identification) information while in transit to the certifying authority.

B. The certifying authority verifies the senders signature on the key and ID. This ensures that the sender is trustworthy.

C. The certifying authority signs the public key and ID with the certifying authority key, creating a certificate.

D. The sender verifies the key, ID, and the certifying authority signature.

E. The applicant publishes the certificate.

If the user's secret key becomes compromised, the certificate associated with the public key must be revoked. The certifying authorities also keep certificate revocation lists that are accessible to the users/parties of the system.

When created in 1970, certificates were conceived as one-time assertions of public keys. They were put in practice in an X.509 directory, which provided the evidence of a person's identity. X.509 is actually a standard for digital certificates. The X.509 recommendation specifies the exact syntax for a certificate that can link a public key to an X.500 DN (distinguished name), where a trusted third party is also identified by X.500 DN.

The X.500 are recommendations for distinguished name were based on the idea of a single global distributed database containing objects representing people and processes. The objects are arranged structurally and top-down. A typical distinguished name component has Country (C), State or Provinces (SP), Locality (L), Organizational Unit (OU), and Common Name (CN). X.509 v3 added support for other name forms such as e-mail addresses, DNS names, URLs, and IP addresses.

Public key certificates constitute the basis for a systematic approach to public-key distribution, which is indefinitely scalable, keeps the burden on the system users to a manageable level, and

has uniform and easily controllable security characteristics. It is widely used in all the payment protocols. They are primarily used for systematic authentication and verification. The novelty of the system lies in the fact that it is not entirely necessary to know the client to trust him. If a client holds a valid certificate from a valid root which can be trusted, the transactions can be accepted.

# Appendix B

# Electronic Cash

Electronic cash are the collection of bits and numbers crafted to act as cash surrogate on the Internet. Any successful electronic cash system on the Web must include nearly all the features offered by cash. Electronic cash offers the benefit of cash by offering anonymity, on- or off-line payment, guaranteed payment, no transaction charge and convenience. Electronic cash must employ strong encryption mechanisms making the cash secure.

One of the first companies to launch electronic cash payment scheme was DigiCash. In the year 1995, the Mark Twain bank in St. Louis, Missouri and EUNet in Finland started to use DigiCash software to support real accounts.

## B.1 Model of Electronic Cash

A generalized model of Electronic Cash system is shown in figure 4.1:

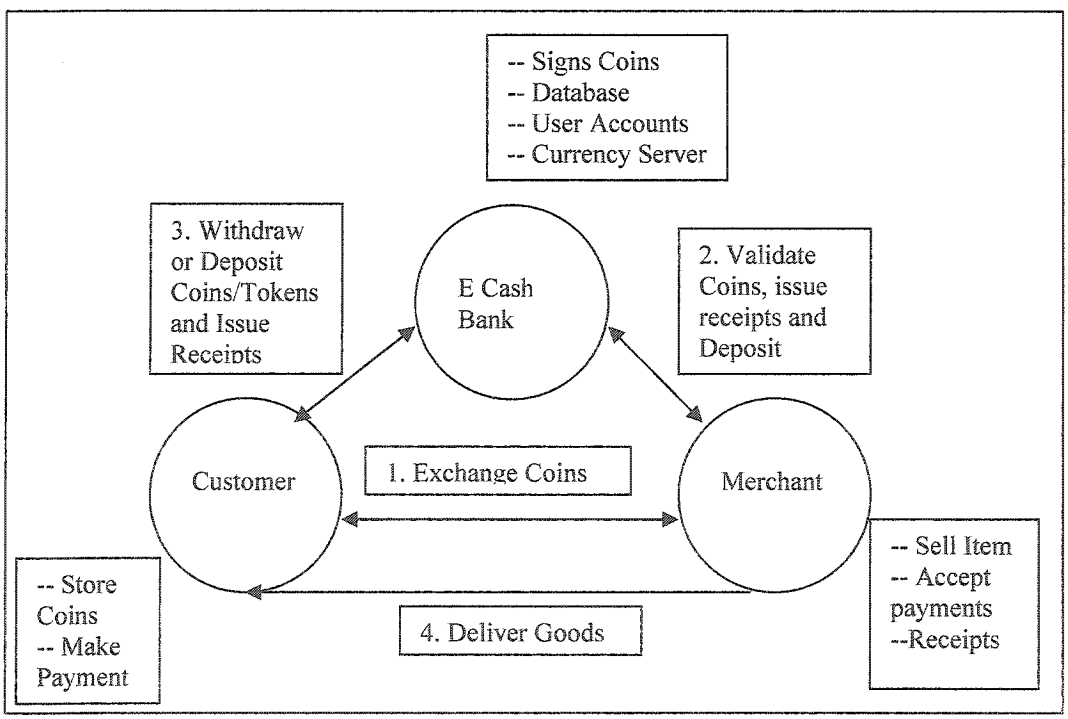



**Figure B.1 Electronic cash model**

Electronic cash differs from other forms of electronic payments by the fact that the customer has nothing to do with the bank at the time of payment of coins or tokens to the merchant. The electronic coins or tokens are a piece of data representing monetary value within an electronic cash system. The banks role is when the merchants deposit the tokens or coins in the bank, they verify the payment and could trace the whole chain and also check for double spending, digital signature and expiration date. Some of the banks maintain an extensive database of the electronic coins spent by the customer for further audit and security.

Until now, both the customer and merchant must have accounts at the same E cash bank. Another bank will not accept coins or tokens obtained from one bank. As the use of E cash becomes more wide spread, it is likely that third parties might exchange coins from different banks or banks might provide this exchange themselves.

The transaction usually proceeds as follows as shown in figure 4.1:
Before any transaction takes place, the two parties (customer and the merchant) establish a secure channel. This might be created if the recipient has published a public key that the spender can use to initiate the transaction. Alternatively, it may be done on an anonymous basis by using Diffe-Hellman key exchange to create a pair of keys. They may also employ a customized Internet draft, which might include the version of the software, the transaction no., and date, the details of transaction, e-mail ID of the client, customer ID, customer signature, public key and other personal details to identify the customer and facilitate smooth transaction. However, all the important details such as e-mail, ID of client, signature are encoded with DES and this DES key is encrypted with a session key which might in turn be encrypted with one of the public keys. CyberCash uses RSA encryption with 768-bit key. When the merchant and customer agree on the terms of sale, the merchant sends customer a receipt of the things he or she will get and prices.

1. The beginning of the transaction.

   The customer accepts the receipt from the merchant, bundles up the coins or tokens and encrypts them with the secure channel's encrypt mechanism as

established between customer and the merchant or with the private key of the customer and sends it to the merchant.

2. The merchant gets this packet and adds its own digital signature or private key.

   The merchant checks the signature with the correct certificate for the currency server that generated the coins. The merchant adds its own signature by appending the merchant ID number. The merchant also encrypts the message with the public key of the currency server before sending it to the banks currency server.

3. The bank's currency server checks for the digital signature of the customer and merchant to verify the authenticity, the availability of coins, and the correct amount and makes sure, that they have not been spent before.

   The currency server decrypts the information from the merchant and checks for the validity of the coins, if the coins haven't been spent before it retires the coins. It then sends an authorization to the merchant as well as a receipt to the customer along with a session ID encrypted in respective public keys of the merchant and customer.

4. The merchant and customer receive the encrypted message.

   Upon the successful authorization, the merchant starts the delivery process of the goods. The merchant may also send the customer a receipt signed with its digital signature guaranteeing the contents.

The return receipt includes all the information about the transaction. As the anonymity in these exchanges are limited. The merchant does not know the identity of the customer nor is there any way for him to find out directly.

We now compare two examples of electronic cash payment systems namely, NetCash and Ecash and highlight the results in table 4.1. These systems were the pioneers of digital cash. Ecash was

even launched commercially for a brief period. After analyzing the systems, we will discuss the strengths and weaknesses of electronic cash in table 4.2.

## B.2 Electronic Cash Payment Systems

Some of the most pioneering Electronic cash systems in the market today are as follows:

1. NetCash [23]

   B.Clifford Neuman and Gennady Medvinsky at the Information Sciences Institute at the University of Southern California designed NetCash. NetCash is a cash system that offers a strong degree of anonymity that can only be broken by the bank. The system has not been implemented so far. The demonstration software is available for some UNIX machines, but not for the most general machines on the market. The digital coins are collections of bits with serial numbers that are guaranteed by the bank's digital signature. The designers endeavored to create a system that is reliable, anonymous, secure against counterfeiting and scalable. The system itself is not secure when the payees are off-line.

   There are significant differences in the level of anonymity, though, with the NetCash system. The protocols are simpler and this allows some banks to track the spending of their customers if they choose. However, they argue that the banks could contractually be barred from keeping the records necessary to unravel the network of transactions and trace people's habit. Some banks might make this anonymity barrier a selling point and advertise their services based upon it.

   The currency server of the net cash server is designed to act as a bank surrogate and performs all the operations. It acts as a mint for digital money. The NetCash system proposes that the government maintain a central certificate authority that would bind up the public key for a currency server and seal it with the government's digital signature.

The coins can be exchanged through different protocols, but this basic two-step response is often adequate:

1. The customer would send the currency server his coins and the instructions on whom to pay or exchange them for new coins and his secret key chosen at random, encrypted with the public key of the bank.
2. The currency server would check the coins and reply the customer back encrypted with the secret key of the customer as given to it.
   Currency server generates coins and each coin has serial number that is unique to that server along with the name of the server, address of the server, expiry date, serial number and the value of the coin. Each coin is encrypted with the issuing server's secret key.

   Coin= {Issuing server, Server's address, Expiry, Serial#, Value}
   Secret Key

During the transaction, each coin is verified by the currency server to prevent double spending. The currency server maintains a list of the serial numbers of every coin issued by it.

2. Ecash [24]

Ecash was one of the first companies to launch a true electronic cash payment system. It was called "digicash" which was by far the most successful electronic payment system because it was launched commercially.

The electronic cash was pioneered by the David Chaum. The structure of digital cash is both account based and token based money. The bank automatically dispenses the coins in sizes that grow exponentially. This system is probably more efficient than the decimal-based system we use today, but it does increase the number of times someone has to break the bill. The merchants in this system receive no anonymity, as they have to turn the coins in immediately upon receipt. The Ecash coins or also known as "tokens" are used as follows:

**Generation of Coins**

The software wallet with the clients generates the coins; which are simply bits and pieces of data created with basic digital cash algorithm using blind signatures. The banks sign a different key for different denomination. The denominations also have very large digit serial number and are randomly chosen to prevent that anyone else will use the same serial number.

Now the denominations are sent to the bank for signatures.

**Withdrawal of Coins**

The sender's software wallet chooses a random binding key say "k." Now, by using RSA algorithm the important coin information viz. serial number, are encrypted. It uses the public prime moduli "m," the banks public key "e," i.e. $\text{Serial\#}*r^{e2} \bmod m$.

Here e2 is the specific key issued by the bank for that set of denomination (say 2-cent).

The bank then signs the coin with its 2-cent denomination key pair say "d2."

$(\text{Serial\#}*r^{e2})^{d2} \bmod m$.

The coin is then returned to the sender.

The sender now divides the binding factor out of the coin.

i.e. $(\text{serial\#}*r^{e2})^{d2} \bmod m / r$ and gets the coins with the bank signature on it. The coins are now ready to be used.

**Transaction using Coins**

To allow the signatures to be quickly verified a plain text version of the serial# is included with the coin. Also included is the information such as, value, currency and expiry date in a file called "keyversion."

With this form as described, where a coin can be any signed large number, anyone can generate a large random number and apply the bank public key to this value to get another large number. This is possible because of the inverse relationship of RSA algorithm. The part of reason is that the serial numbers are completely random and there is no way to distinguish a genuine signed serial number from one created using the RSA inverse property.

To prevent this, serial# (not the one in the plain text) is run through a Hash function (say SHA). Thus, the Ecash systems are further strengthened by using a redundancy-adding function in combination with a one-way hash function.

To prevent double spending the Ecash bank must store a database of spent coins. Before any transactions takes place the bank must match the database to ensure the coins have not been spent before. Also, in theory people can exchange the disks, with all of the cash stored in them. However, anyone doing so risks losing money because there are no cryptographic protections against double payment in this system.

The transaction occurs between the merchant's machine and Digi-Cash wallet running on the customer's computer. Both need to have full IP addresses and Internet access. The request triggers a script that runs a program that manages the transaction. This program dials up the ecash wallet running on the customer's machine and asks for some cash.
Then, the wallet software asks for the confirmation from the user. Thus the merchant is paid.

## B. 3 Comparison

The comparison between NetCash and Ecash in Digital cash systems is tabulated in table 4.1:

| Criteria | NetCash | Ecash |
|---|---|---|
| Market release | NO | YES, 1995 -1998 |
| Security | Public/Private keys and Digital signatures | Public/Private keys, blind signatures, SHA , Redundancy |
| Prevention of Double spending | Database matching | Database matching |
| Need for Certification Authority | YES | YES |
| Customer Anonymity | Limited (only through proxy) | Total |
| Peer-to-peer pay | YES | YES |
| Merchant's anonymity | YES (if bank agrees) | NO (Contact bank for validity) |

**Table B.1 Comparison between NetCash and Ecash**

NetCash was never released as a commercial product. Mark Twain Bank in St. Louis, Missouri released Ecash in the market. It was in operation from 1995 to 1998. Both of the electronic cash relies on high-end encryption. However, Ecash has a clear edge over NetCash when it comes to security as it uses dual signatures and redundancy algorithms.

Both of them use, the conventional database matching to check for double spending. NetCash as well as Ecash needs certificate authority to maintain the authenticity of the originator. Both the systems allow peer-to-peer pay however, it should be noted that, as double spending could not be performed while the currency is offline.

## B. 4 Strengths and weaknesses of electronic cash

| | Consumer | Merchant |
|---|---|---|
| Strength | Anonymous, secure, quick, no information is given to merchant and maintains privacy | Quick hassle free transactions, immediate payment, accept small payments. |
| Weakness | Need to have valid certificate (NetCash), robust and resource intensive protocol, install software wallet, update certificate revocation list (NetCash) | No consumer information or details are stored, no anonymity, need to have certificate and update certificate lists (NetCash), verify from bank immediately. |

**Table B.2 Strengths and weaknesses of E-cash**

# Appendix C

## Electronic Cheque

An electronic cheque or e-cheque is based on the idea that electronic documents can be substituted for paper and that public key cryptographic signatures can be serve as surrogate for hand written ones.

The payer writes an e-cheque by structuring an electronic document with the information legally required to be in a cheque and cryptographically signs it using his digital signatures. Then, before he sends it he runs a hash algorithm and sends it over the network.

The payee verifies the e-cheque, verifies the payer's signature, writes out a deposit, and signs the deposit and forwards it to his bank. The bank in turn verifies both payees and payer's signature, credits the payee's account, and forwards the cheque for clearing and settlement.

## C.1 Model of Electronic Cheque

A generalized diagram of electronic cheque as presented by NACHA [25] is shown in figure C.1:

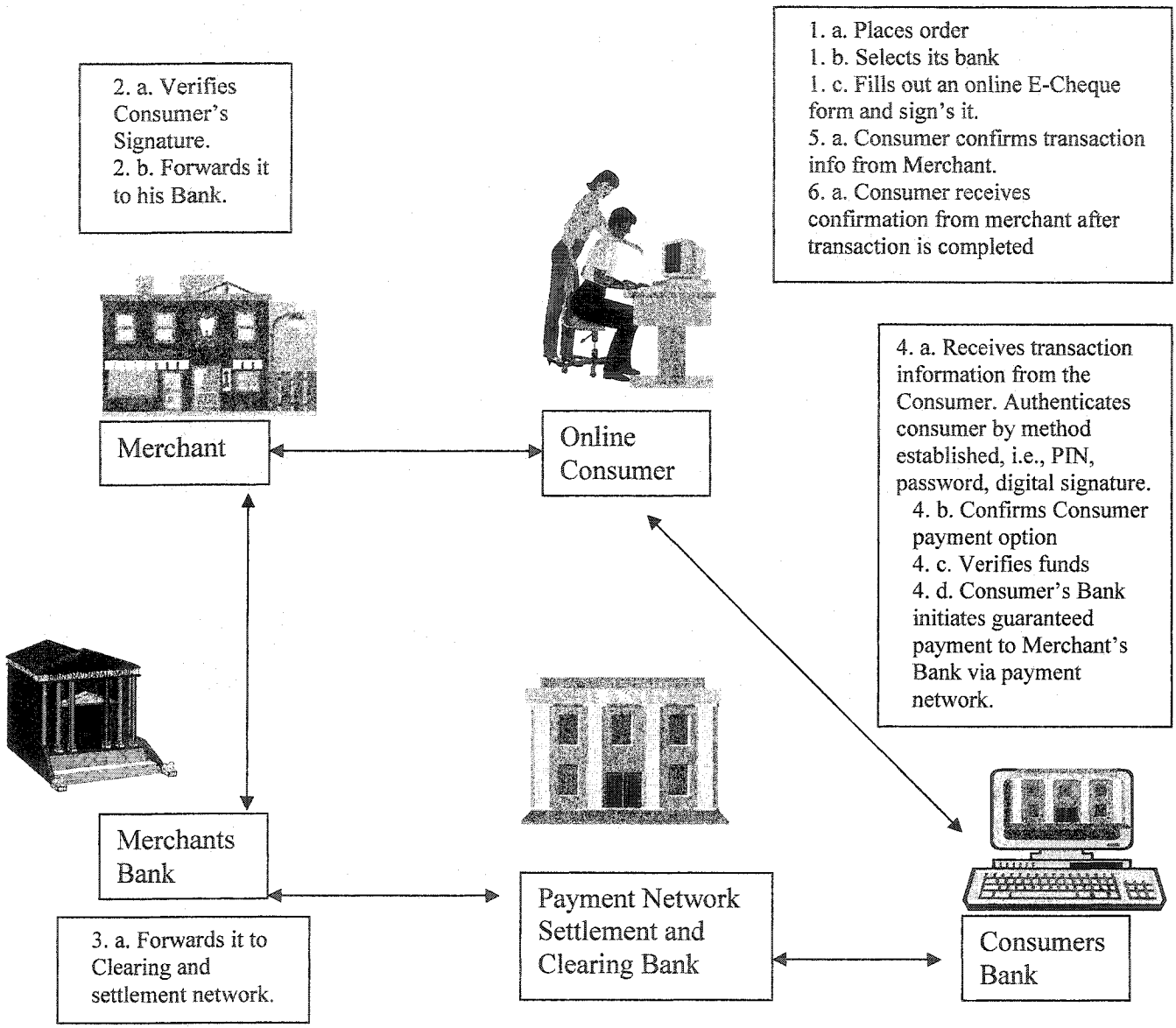



**Figure C.1 A general model of electronic cheque transaction [25]**

One significant advantage of e-cheque over paper one is that the e-cheque can be verified at all points (merchant, at merchant's bank, at issuer's bank), while the paper cheques with handwritten signatures are verified only at the issuer's bank. In addition, it is very hard to forge an electronic cheque as the use of hash functions makes is infeasible for someone to tamper with the file in any way without tampering the final hash value. The electronic cheque has been growing in popularity. According to NACHA survey, in the year 2002, the total number of

electronic cheque transaction numbered, 517.74 Million transactions [26]. The total dollar volume of e-cheque transactions was $ 101.54 billion, representing 0.42% of all ACH volume (24.4 trillion) in 2002. Some of the pioneering electronic cheque systems were "NetBill [27]," "NetCheque," "CheckFree," and "NetChex."

## C.2 Electronic Cheque Payment Systems

In the following, we review NetCheque, CheckFree and NetChex cheque systems. These are the pioneering and widely used electronic Cheque systems. After, discussing their features and advantages, we present a comparison between them in table C.1 followed by a discussion of overall strength and weaknesses of the electronic cheque payment system.

1. NetCheque [28]

   NetCheque system is a non-anonymous system that was developed by a team at the Information Sciences Institute (ISI) at the University of Southern California. The designers wanted it to scale well and offer low-cost transactions that would be appropriate to allow micro billing. The NetCheque system relies upon the Kerberos system. Trust emerges for the central server, which knows both the client and server.

   When the customer wants to sign the cheque, they call for a ticket from the Kerberos server. This initial call up tells the server that the customer wants to make a secure connection between him and the recipient. The server returns a ticket that contains an encrypted copy of a secret key between the customer and recipient. The secret key is encrypted in two ways, once by the customer's password and second time by recipient's password.

   The customer then prepares the hash of the details of the cheque and appends it to the secret key as issued by the server. The message is now sent to the recipient over a secure network.

The secure hash algorithm is intended to prevent someone from changing content of any data files. Anyone can verify the signature by decrypting the signature with the corresponding public key and also computing the hash function of the file.

The recipient decrypts the message, verifies the hash, and endorses it as it could have come from no one else but the consumer. Then, he forwards the endorsed cheque to the customer's bank.

2. CheckFree[29]

CheckFree is a system specializing in paying any type of bills online, using cheque. According to their press release (Atlanta, April 20, 2004), the company processed more than 152.2 million transactions for the quarter (third fiscal of 2004).

CheckFree guarantees the bill payment in typically four to five business days. More than 75% of the CheckFree's payments are made electronically. The remainder of payments are mailed by cheque, generally to smaller merchants. It is also worthy to mention that in case of any late payment, the CheckFree will bear all the late charges (up to $ 50) as long as the transaction is scheduled in accordance with the service terms and conditions.

CheckFree typically require the consumer's e-mail address, the consumer chequebook, driving license, the Social Security number and a recent bill which we want to pay online to sign up. They provide the convenience of writing up an online cheque to anyone whom we pay today with paper cheque.

This system provides no anonymity but is certainly more accountable than many existing systems. Also, its existence for a decade and its collaboration with many companies [30] in providing billing supports its credibility.

CheckFree uses the client's user name and password to identify the client. The name and password is encrypted using SSL while it goes over network. The CheckFree also features to automatically logout a client after a while if the account is unused.

3. NetChex[31]

NetChex was introduced by Universal Payment Solutions. NetChex looks exactly like paper cheque except that the customer fills it out online [32]. NetChex features VeriChex and IdentiChex [33].

At the time of signing up for an account, they need customers to provide many personal details such as SSN (social security number), a verifiable address, a verifiable phone number, driving license and an ABA routing number (given by bank).

At the time of writing off a cheque, they match all this information using an IdentiChex and VeriChex. IdentiChex does real time matching of the customers details including name, address, date of birth, phone number, driving license number, SSN and MICR (Magnetic Ink Character Recognition)[34] data. VeriChex allows the system to determine whether an account is valid and if that account is overdrawn, frozen or closed. The database is updated daily and is always kept online.

NetChex is completely compatible with current banking infrastructure and does not replace any components of the existing system. NetChex ensures the privacy of the users by the using symmetric key encryption with dynamically generated keys. By this method, each transaction rests on the preceding transaction.

## C.3 Comparison

The comparison between NetCheque, CheckFree and NetChex are as follows:

| Criteria | NetCheque | CheckFree | NetChex |
|---|---|---|---|
| Market release | NO | YES | YES |
| Security | Kerberos (Symmetric Key) | SSL | VeriChex, IdentiChex, Symmetric Key |
| Need for Certification Authority | Kerberos | YES | NO |
| Customer Anonymity | NO | NO | NO |
| Merchant's anonymity | NO (Contact bank for validity) | NO | NO |
| Peer-to-peer pay | YES | YES | YES |

**Table C.1 Comparison between NetCheque, CheckFree and NetChex**

NetCheque has not been released in the market. However, the license of the software could be brought by contacting appropriate authorities. CheckFree and NetChex have been released in the market and are in operation.

NetCheque relies on Kerberos server authentication security. Thus, the user must call for the ticket before he indulges in the transaction. CheckFree relies on SSL for security. And NetChex offers variety of propriety security features including VeriChex, IdentiChex.

NetCheque is based on Kerberos server authentication technology and thus, its users does not need to have a certificate. There is a new session key generated for every transaction. CheckFree based on SSL needs its users to have certificate. We could not evaluate the NetChex security mechanisms. They use their own propriety mechanism, which does not involve any certificate authority.

NetCheque, CheckFree, NetChex users are offered no anonymity. However, anonymity is replaced by accountability.

Electronic Cheques allows pay between its peers. In NetCheque, both the parties must posse's valid ticket at the time of transaction. CheckFree allows its customers to write cheque to anyone. If the recipient cannot receive the cheque electronically then, the checkfree mails them a printed copy of the cheque. NetChex similarly, allows users to pay to anyone.

## C.4 Strengths and weaknesses of Electronic Cheques

| | Consumer | Merchant |
|---|---|---|
| Strength | Secure, pay to anyone (who has account with the bank), ubiquity, no need to install wallet software. | Quick hassle free transaction, no fraud, immediate approval from bank |
| Weakness | No anonymity, need to have valid certificate (CheckFree), robust and resource intensive protocol (SSL), no immediate payment, not suitable for small value payments. | No anonymity, need to have certificate and update certificate lists (SSL), takes long time (typically 2-4 days for transfer), and cannot accept small value payments. |

**Table C.2 Strengths and weaknesses of Electronic Cheques**

# Appendix D

## Smart Cards

Smart card is any device with more memory than a magnetic strip and is capable of allowing monetary transactions. Nevertheless, technically speaking, a "true smart card" has not only more memory (16 to 64 KB), but also an onboard smart processor or a microchip within the device. The concept of smart card is not new. It dates back to 1968, when two German inventors, Juergen Dethloff and Helmut Grottrup, patented the idea of an integrated circuit in a plastic card, what they called "identificand" (identity card) [35]. In Japan in 1970, a patent for a contact-less card was registered. The first U.S patent to be issued for a smart card went to Roland Moreno in 1975.

A smart card has a microprocessor or memory chip embedded in it, which, when coupled with the card reader, has the processing power to serve many different applications. It can be used as an access-control device and can be used to distribute business or personal data to appropriate users. Another application is to provide users with the ability to make purchases or to exchange value. Smart cards provide data portability, security, and convenience.

Smart cards actually offer more security and confidentiality during online transactions than other financial information or transaction storage vehicles, making them highly desirable for e-commerce. One of the novelties of a smart card is that it possesses computational power within the card itself and therefore provides greater security during transactions.

With credit card fraud already costing billions world wide, there was a need for a new mechanism to facilitate financial transactions securely. True smart cards (cards that contain a microprocessor) are hindered by the fact that they have slow processors and typically possess only a few kilobytes of RAM. However, a new smart card chip is currently being tested that contains 1 MB of RAM [36] and houses special circuitry to perform cryptographic operations such as RSA public key encryption, signatures, and authentication. Unlike magnetic stripe-based cards (like most credit cards today), which can be compromised for the purpose of criminal

activity, smart cards are difficult to duplicate. Therefore, with the growth of e-commerce and the need for ever more security, the smart card will grow in popularity.

## D.1 Types of smart cards

There are two general categories of smart cards, "contact" and "contact-less." The contact smart card requires insertion into a smart card reader. The contact-less one just needs to be close to the reader, deriving its power from the electromagnetic signal from the reader. Typically, the distance between the card and the reader does not have to be less than 2 to 5 cm. The contact-less card is ideal for mass transit, or where a very quick interface is needed such as gas stations, parking ticket systems, or for identification purposes. As reported by Smart Card Alliance (a non-profit group which is working to accelerate the widespread acceptance of smart card technology [37]) two emerging categories are combi cards and hybrid cards. A combi card has two interfaces i.e., both contact and contact-less. On the other hand, a hybrid card has two chips, one supporting contact technology, and other supporting contact-less technology. A combi card combines the two features (contact and contact-less) with a very high level of security. Smart cards can be divided in the following categories:

- Memory Cards

  Memory cards contain EEPROM (Electrically Erasable Programmable Read only Memory). Memory cards simply store data and can be viewed as small floppy disks with optional security. They are usually based on $I^2C$ (serial memory) bus. Memory cards rely on the security of the card reader for their processing, and are ideal only when the security requirements are low to medium. A layout of a typical memory card is figure D.1:

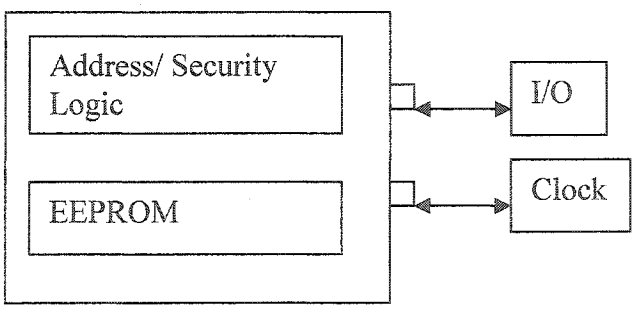



**Figure D.1 Layout of a memory card[38]**

- Microprocessor cards

  A microprocessor card contains a microprocessor chip and can add, delete and otherwise manipulate information in its memory. They contain an operating system and can perform a wide range of operations using an input/output port. Typically a microprocessor card consists of a CPU (central processing unit), ROM (read only memory), EEPROM, or EPROM. A detailed layout of the microprocessor card as formulatd by Gemplus [38] is drawn in figure D.2:

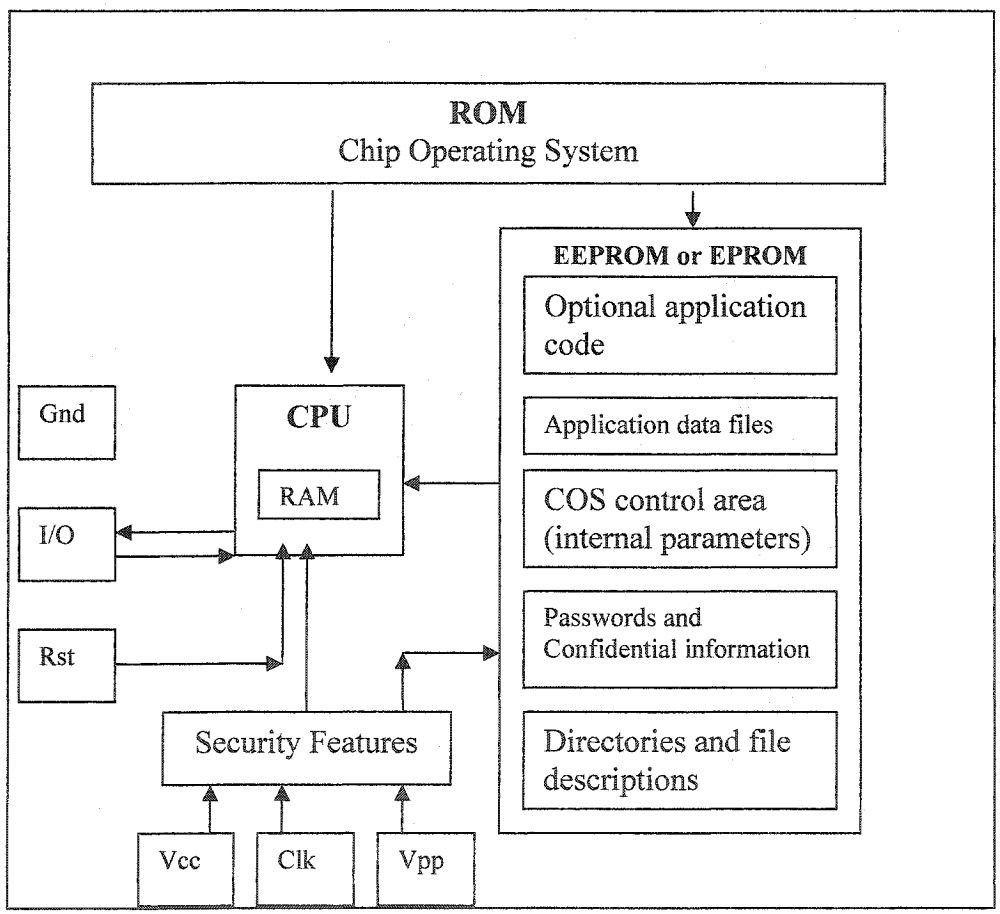



**Figure D.2 A typical layout of Microprocessor Smart Card [38]**

LEGEND: Gnd is the ground. I/O is the input and output port. Rst is the reset signal for the CPU. Vcc is the supply voltage and Vpp is the pump voltage or peak-to-peak voltage for writing in the RAM. ROM is read only memory; it generally houses the chip operating system and cannot be rewritten or modified in anyway.

The operating system interacts with other components of the chip. EEPROM or EPROM (figure D.2) bear other essential codes and files. They can be modified or changed. EEPROM has typically 10,000 write/erase cycles.

## D.2 Standardization

Smart cards are governed by ISO 7816 standards [39].

ISO 7816-1(1998): Defines physical characteristics, including typical smart card size. Amended in 2003.

ISO 7816-2(1999): Defines location, dimension, and size of the electronic contacts.

ISO 7816-3(1997): Defines electrical signals and transmission protocols. Amended in 2002.

ISO 7816-4(1995): Defines, in part, the communication protocols among applications. Amended in 1997.

ISO 7816-5(1994): Amended in 1996.

ISO 7816-6(1996): Defines inter-industry data elements. Amended in 2000 and corollary issued in 1998.

ISO 7816-7(1999): Defines standards for query language commands.

ISO 7816-8(1999): Standardizes security-related commands.

ISO 7816-9(2000): Standardizes additional inter-industry commands and security attributes.

ISO 7816-10(1999): Electronic signals and answer to reset for synchronous cards.

ISO 7816-15(2004): Defines cryptographic information.

Like the operating system in a PC, smart cards with chips inside them also need operating systems. Several smart card operating systems exist today. Three major emerging multi-application smart card operating systems are Multos [40], JavaCard, and Windows. For the card to work it needs a mechanism to exchange and manage monetary value; this is done by software called electronic purses or e-purse. The purses store pre-paid monetary value directly on the smart card. Some prominent names are Mondex [41], Visa Cash [42], Proton, and Danmont [43]. The first standard to emerge among the e-purse was CEPS (common electronic purse specification), introduced by CEPSCO, LLC.

Launched in October 1999, CEPS [44-45] defines standards for electronic purse systems around the world and features compatibility with EMV (Europay-MasterCard-Visa) specifications, which have fast become the *de facto* standard in banking with integrated circuit cards while maintaining accountability and auditability. Interoperability is essential to any payment system.. Along with compatibility with EMV specifications for smart cards, CEPS also defines the requirements for an interoperable card application, the card-to-terminal interface, the terminal application for point-of-sale and load transactions, data elements, and recommended message formats for transaction processing. CEPS also provide functional requirements for electronic purse scheme participants and uses public key cryptography for enhanced security. CEPS also establishes the certification process and maintain security profiles.

Proton World [46] was launched 1998 in Belgian and created by big corporations around the world including American Express, Visa International, Banksys (the Belgian EFT network provider) and ERG Interpay. With its alliance, including MeT (Mobile Transactions, a consortium founded by Motorola, Ericsson, and Nokia to establish a framework for secure mobile transactions), JavaCard Forum (a discussion and development group endorsed by Sun Microsystems) and UITP (International Association of Public Transport, an association of urban and regional passenger transport operators), Proton hopes to be a big player in the industry. It also implements the EMV international specifications for credit/debit cards. Some of their new security products include a fingerprint verification module, developed by Keyware Technologies, which reads fingerprints, compares them with bio prints stored on the Proton card, and then send encrypted data to the Proton terminal.

Currently, having licensed in 24 countries, over 35 million cards in circulation, and over 226 million purchases made, the Proton R3 e-purse is the most widely used e-purse product in the world [47].

The EMV [48] was formed in February 1999, by Europay international, MasterCard International, and Visa International. Its primary objective was to manage, maintain, and enhance

the EMV integrated circuit card specification for payment systems. The specifications are defined in four volumes.

Smart cards have been employed in a variety of applications. One recent application is Internet transactions. Two big players in the smart card arena are Mondex and American Express., American Express "Blue," utilizes java technology [49]. After, discussing the two cards, we will analyze them (table D.1) and end the chapter with strength and weakness of smart cards (table D.3). We will also compare the stand-alone and authentication-based cards (table D.2).

## *D.3 Smart Card Systems*

1. "Blue" From American Express

   American Express launched its smart chip "Blue" card on September 8, 1999 employing Java technology. It is a contact card with a microprocessor chip embedded in it. Thus, it can be used as a credit card and contains an electronic certificate to verify the points used to make purchases in conventional shops. American Express is offering a free smart card reader for its users.

   The card is connected using a smart card reader. The smart card reader uniquely identifies the card member and thus provides additional security online. It also comes with a Web tool called ID Keeper, which makes online shopping easy. The ID Keeper stores URLs, log-ins, and personal data on the smart card. ID Keeper comes with utility, which detects the card as soon as it is inserted in the reader and brings out the appropriate login information for each site.

   Another innovative tool offered by Blue is "Private Payments" [50]. Private payments enable American Express Card members to use a temporary credit card number with limited validity instead of their actual number. Therefore, the actual credit card number never goes through the transaction. The validity of the number is anywhere from 30 to 67 days. Before the private payments can be used the customer has to request a new number from the private payment's page. The

charges are billed to their actual card. The temporary card numbers are indistinguishable from the original ones so the merchants never find out the actual number.

The card is based on Java and contains multiple applets. These applets can access packages and services from other applets. These applets can be rapidly and securely built, tested, and deployed, providing an attractive choice for many developers. "Blue" has been issued in both Java and Multos version. The electronic purse of blue is CEPS compliant and also supports Proton.

2. "Multos 4" Card by GemPlus [40 & 51]

Gemplus was founded in 1988 and offers smart card solutions and a variety of products in the industry. It began its operation by issuing phone cards and SIM cards. After joining smart card forums in 1993, it began its production of smart cards. According to Gartner-Dataquest, Gemplus is number one in the world in smart card shipments, with a 35% market share in 2001.

Gemplus offers a range of products, which include smart cards and smart card readers and accessories [52]. Most of their cards for banking application are java-based cards, which comply with CEPS.

One of the products by GemPlus is Multos 4, which is based on the Mondex e-purse scheme. Mondex was developed in 1990 at NatWest, a major banking organization from the United Kingdom.MasterCard bought a 51% stake in Mondex in 1997. In 2001, MasterCard announced its intentions to own Mondex.

Mondex is an electronic payment system based on smart card technology. Mondex is structured around six constituents, which operate according to various roles. Mondex International, a subsidiary of MasterCard International, operates, owns, and administers the scheme. They license the use of the scheme to franchises acting in different countries. These franchises issue, control and

redeem electronic cash denominated in a given currency. The manufacturers are licensed to provide equipment to any Mondex scheme participant. The equipment they wish to sell will typically undergo a 'type-test' to ensure compatibility with Mondex specifications.

The card is charged at the time of issue. Charging can also be done through specially equipped ATMs, card telephones, mobile phones, or Internet. Mondex cash is digitally stored on a reloadable and highly secure microprocessor computer chip.

One of the distinct features of Mondex is that there is no need for online dialogue with the bank to verify the transfer. Mondex uniquely combines high security with person-to-person payment functionality; this means no third party intermediary clears or processes every transaction. Mondex can be transferred chip-to-chip using the Mondex wallet, over a telephone line, over the Internet, or wirelessly.

## D.4 Comparative Evaluation

A comparison among various smart cards follows:

| **Criteria** | **Blue** | **Multos 4** |
|---|---|---|
| Market release | YES | YES |
| Electronic Purse Supported | Proton/CEPS | Mondex |
| Operating System | Multos/Java | Multos |
| Security | Java Security | Proprietary |
| Need for Certification Authority | YES | NO |
| Customer Anonymity | NO (If used as credit card) | YES |
| Peer-To-Peer payment | NO | YES |

**Table D.1 Comparative evaluation between Blue and Multos 4**

American Express planned to spend about $45 million in advertising, though they would not comment on demand for the card or the number issued. Mondex has been in testing since 1992, but was only released in 1999.

The security in "Blue" is Java based. However, Mondex never released its security for the protocol publicly. There is a definite need for a certifying authority in "Blue," which is typically the American Express bank or one of its subsidiaries. There is no need for certifying authority in Multos 4.

Blue supports both Proton and CEPS electronic purses. American Express is one of the first accepters of Proton. One of the big advantages of Multos over Blue is Mondex's ability to pay person-to-person. Customers are anonymous to the merchant in Mondex. However, all transactions have to be approved by the bank in Blue, since the card is mostly used as a credit card.

Smart cards are gradually becoming popular in e-commerce applications. Along with e-commerce applications, smart cards are also gaining popularity in general retail businesses and for small value transactions. However, one very troublesome aspect of the small purchase transactions is the transaction cost involved. Most of the retailers would not accept credit card transactions less than two dollars. Therefore, there is a definite need for a smart card which can accept small value transactions (viz. buying a newspaper, a cup of coffee, parking machines, public transport) at an acceptable cost. These cards are prepaid value cards, can be used without any link with the issuers at the time of payment, and can be loaded when necessary. We will refer them as "stand alone smart cards."

One such e-purse was introduced by Visa and named Visa Cash. Introduced in April 1995, it went through pilot project around the world before being implemented. It was targeted to replace currency and coins under US $10. Visa Cash has been implemented in both proprietary and open-platform cards. They come with both disposable and reloadable features. Disposable cards are disposed of after the amount is used up, whereas the reloadable ones can be loaded by special ATM machines.

Unlike the systems discussed above (Blue and Multos 4), Visa Cash works without maintaining a robust channel between the merchant and the bank. Visa Cash is a secure application module (SAM) based system and requires merchant terminals that contain card readers. To process a

transaction, after validating the customer's card, the protocol sends encrypted details to the card to activate the e-purse software. It then verifies the response from the card, making sure the correct amount was deducted, and issues a log and a confirmation to the customer. All the transaction information is stored in the terminal's memory in the SAM in case the terminal fails and therefore, the value can be recovered. The SAM also manages the security details to ensure that a transaction log cannot be fraudulently modified.

In October 2000, CardBASE Technologies [53], a provider of smart card solutions, launched VCEPS (Visa Cash Electronic Purse Specifications) which is CEPS-compliant and therefore, created an opportunity to offer a truly global, interoperable product.

Along with financial institution members, Visa Cash has formed relationships with technology partners around the world to pursue the transport market. It is trying to develop an open electronic purse scheme for automatic fare collection among transport agencies.

Therefore, it becomes essential to compare the e-commerce based payments to retail payments. For the smart card to widely popular in the market, it not only needs to prove itself in the e-commerce arena but also in small value transactions.

## D.5 Comparative Evaluation

A comparison between small value smart cards and e-commerce based smart cards follows:

| Criteria | Stand-alone Smart Card | Authentication-based Card |
|---|---|---|
| Market release | YES (e.g. Visa Cash, Mondex) | YES (ex. Multos4, Blue) |
| Electronic Purse Supported | Visa Cash/CEPS | Mondex, Proton, CEPS |
| EMV Compliant | YES | YES |
| Security | Triple Des | Propriety, RSA, DES, DSA, Certificate, DSA |
| Need for Certification Authority | No | YES |
| ISO 7816 Compliant | YES | YES |
| Ease of Use | Easy (Just swipe or come close for contact-less ones) | Clumsy (Enter PIN and accept transaction) |
| Acceptability | NO (Its not widely popular) | YES (The merchants already have a mechanism to verify credit card) |
| Customer Anonymity | YES | NO (If used as credit card) |
| Monetary value Recovery | NO (If Lost) | YES |
| Need for PIN | NO | YES |
| Peer-Peer payment | NO | YES (In Mondex) |

**Table D.2 Comparative evaluation between stand-alone and authentication-based cards**

Visa Cash has been released in the market but is currently only accepted at terminals, which display the Visa Cash logo. Thus, Visa Cash is an alternative to cash and exists alongside traditional credit and debit cards. Visa Cash offers convenience and flexibility; credit cards offer such benefits as revolving credit and interest-free periods.

Stand-alone cards also support CEPS and EMV standards, along with authentication-based cards. As stand-alone cards don't need to verify the individual's identity, they don't support a very high encryption. They just need security just in case someone tries to transfer the information from the card to another card. There is no certification authority in stand-alone cards as the merchant's just need to verify the authenticity of the card.

Stand-alone cards are certainly easier to use. They are quick, fast, and there is no need to enter a PIN. Some of the new generations of stand-alone cards (EZPay) are contact-less and therefore, the transaction is very quick, without any hassle and without any human intervention.

Stand-alone credit cards can only be purchased at a terminal and can only be used at POS terminals, which accept them. Many pilot projects are running, especially in public transport systems. Authentication-based cards, on the other hand, use already existing protocols (for credit cards) and therefore, seem to integrate very easily.

Customers are totally anonymous in stand-alone cards and there is no check to verify the identity of the user. In authentication-based cards, the bank must know who the person is before endorsing the transaction. Once the stand-alone card is lost, its value cannot be recovered to the customer. Anyone who finds it can use it for purchases. However, with authentication-based cards, it's very difficult to use someone else to use the card as the card is PIN-protected.

## D.7 Strengths and weaknesses of smart cards

| | Consumer | Merchant |
|---|---|---|
| Strengths | Secure, pay to anyone (must have reader if using Mondex), ubiquity, no need to install wallet software, anonymity. | Quick hassle-free transaction, no fraud (if not used as credit card), immediate payment, small value transaction |
| Weaknesses | Need to have valid certificate (Blue), need to purchase card reader, no value recovery if card is lost (Mondex). | Need to have certificate and update certificate lists (Blue), purchase card reader (Multos 4). |

**Table D.3 Strengths and weaknesses of smart cards**

# Appendix E

## Credit Cards

Credit cards are very different from other modes of payment because instead of paying right away, the users can build up the credit and pay at some later time. It is based on the model of trust involving the merchant, customer, and the financial institutions.

As outlined previously, the idea of a credit card is not new. Diners Club was formed in 1950, whereas American Express has been in operation since 1958. However, the two dominant credit card companies are Visa and MasterCard. These are non-profit associations that set standards for the issuing banks that actually issue the credit cards and process transactions. Other third parties (called processing centers or clearing houses) usually handle verification of accounts and balances. Credit card issuing banks act as financial intermediaries, minimizing the risk to transacting parties.

### E.1 Advantages

Credit cards offer numerous benefits to the customers over other modes of payment; the most important of all is that the user does not have to have the money in his account before he spends it. Unlike e-cheques, e-cash, or smart cards, where the user needs to have the money in his account before spending it, credit cards offer more convenience. Second is the ease of use. Customers don't have to carry bulky cash or chequebook, or need a computer to run special wallet software. Users can use it to pay online or at a grocery store or a pawnshop—wherever credit cards are accepted. Third, the maximum liability in cases of fraudulent use (once reported lost or stolen) as defined by U.S. federal law is $50 per card. Therefore, the card is deemed safe to use.

### E.2 Security

The majority of credit card numbers are encrypted before they travel online. Several protocols are available to encrypt numbers for online transactions. Some notable ones are SET (secure electronic transactions) and SSL (secure socket layer). SET is newer than SSL. SSL is widely

used. We will analyze these two protocols (table E.1) and present the strength and weakness of the protocols (table E.2 and E.3).

### *E.2.1 SET [54]*

Payment systems and their financial institutions will play a significant role by establishing open specifications for payment card transactions that provide for confidential transmission, authenticate the parties involved, ensure the integrity of the payment instructions for goods and services, order data, and attest the identity of the cardholder and the merchant to each other.

Secure electronic transaction protocol was introduced by two leading proponents, Visa and MasterCard, forming an independent company called Secure Electronic Transactions LLC (SETCo) in December 1997. The first version was released on May 31, 1997. It contained three parts; the first one described the background information and processing flows for SET. The second one contained a programmer's guide. It contained the details of system design, certificate management, and payment system. The third one defined the protocol. It included a chapter on cryptography, message encapsulation, payment messages and its components, handling certificate management, and the ASN (abstract syntax notation): an international standard whose main purpose is the specification of data used in communication protocols.

SET was never intended to be a general purpose payment protocol. It has restricted itself for payment by cards (smart cards and credit cards). It provides confidentiality of information, ensures payment integrity, and authenticates both merchants and cardholders. Its main motivation was to encourage the payment card community to take a leadership position in establishing a secure payment specification while respecting and preserving the relationships between merchants and acquirers and between cardholders and issuers. It also resolved to maintain security and interoperability between the various parties involved.

The following parties are involved in the transaction process.

Cardholder: the customer that has been issued the card. SET ensures that the cardholder's interactions with the merchant and the payment card account information remain confidential.

Issuer: the financial institution that establishes the account of the cardholder and issues the card. The issuer guarantees payment for authorized transactions using the payment card in accordance with payment card brand regulations and local legislation.

Merchant: They offer goods for sale and have a relationship with an acquirer. With SET, the merchant can offer its cardholders secure electronic transactions.

Acquirer: An acquirer is the financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

Payment gateway: A payment gateway is a device operated by an acquirer or a designated third party that processes payment messages, including payment instructions from cardholders.

Brand: Financial institutions have founded payment card brands that protect and advertise the brand, establish and enforce rules for use and acceptance of their payment cards, and provide networks to connect the financial institutions. Brands can also be owned by financial services companies that advertise the brand and establish and enforce rules for use and acceptance of their payment cards. These brands combine the roles of Issuer and Acquirer in interactions with card holders and merchants.

Third Parties: Issuers and acquirers sometimes choose to assign the processing of payment card transactions to third-party processors.

SET [55] employs very high-end security. It makes use of secret-key cryptography, public-key cryptography, digital signatures, message digests, and certificates with trusted third parties. SET employs SHA (secure hash algorithm), which generates 160-bit message digests. The figure E.1 and E.2 shows the summary of the entire encryption and decryption process.

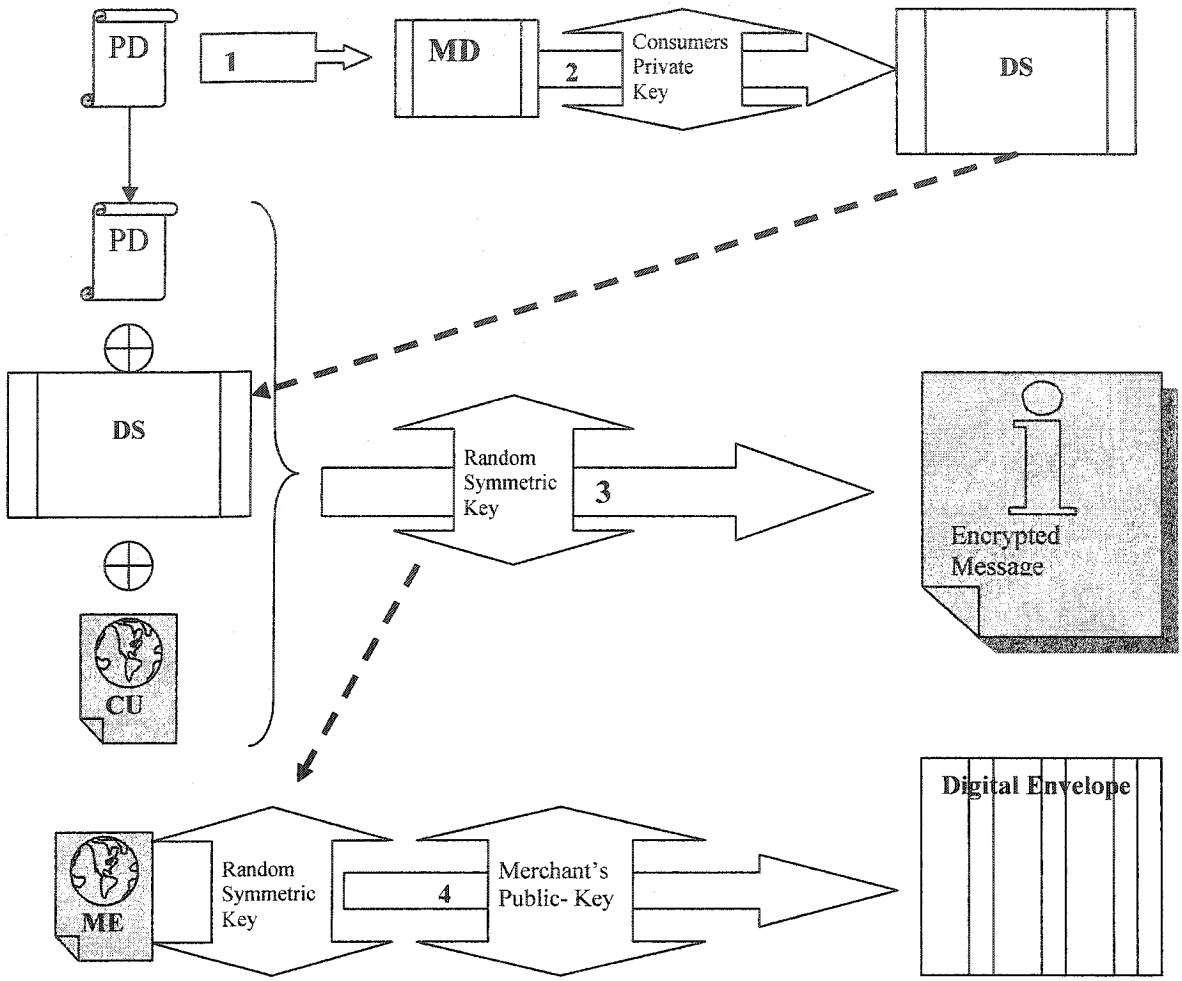



**Figure E.1 Encryption protocol, Based on SET Specification, Book 1: Business Description, version 1.0, May 31, 1997 [54].**

To participate in the SET process, all the parties must have appropriate certificates issued from valid authority. The protocol checks for validity and proper signatures. Then, the protocol checks for proper authorizations and then exchanges purchase instructions and order instructions.

To start the encryption process (figure E.1), first a property description (PD, which consists of credit card numbers and other relevant transaction details), is prepared. The preparation of the property description is outside the scope of the SET protocol. However, the SET payment starts after the cardholder has been presented with a completed and approved order form by the merchants. The participants must publish their "public keys" digitally signed by a "certificate authority" in accordance with the rules of the financial institutions.

Step 1 (as shown in figure E.1):

The customer runs a one-way hash algorithm to produce a unique value called the "message digest" (MD). The message digest acts as a digital fingerprint. The SET protocol typically uses a 160-bit Secure Hash Algorithm.

Step 2:

The message digest is then typically encrypted with the customer's "private key" to form a digital signature of the message digest. The private key is typically generated by using an R.S.A algorithm.

Step 3:

Now, a random symmetric key is generated and is used to encrypt the property description, the signature, and the customer's copy of the certificate. The certificate contains the "public key" of the customer.

Step 4:

The customer now encrypts the symmetric key with the merchant's "public key." The merchant's public key can be verified from his certificate.

Step 5:

The customer sends the encrypted message and the digital envelope to the merchant.

The R.S.A encryption is typically used with a 1,024-bit key and allows interoperability with the messages as defined in a machine-independent format (ASN 1.0). However, with the increase in computation power, 2,048-bit keys are becoming common these days.

The decryption process (figure E.2) starts with the merchant receiving the message from the customer.

Step 6:

Merchant decrypts the "digital envelope" with his private key and obtains the symmetric key.

Step 7:

The encrypted message is now decrypted using the symmetric key and the merchant obtains the customer's certificate, the property description, and the customer's digital signature.

Step 8:

The merchant now decrypts the digital signature of the customer using the public key he obtains from the customer's certificate. He produces the "message digest."

Step 9:

He runs the property description through the same hash algorithm as the customer and obtains the "message digest."

Step 10:

The merchant compares the two "message digests." If they are not the same, he discards them or reports it to the appropriate authority. This step ensures that the message has not been altered on the way. The change of only one word will result in an entirely different message digest.

A pictorial representation of the decryption process is shown in figure E.2:

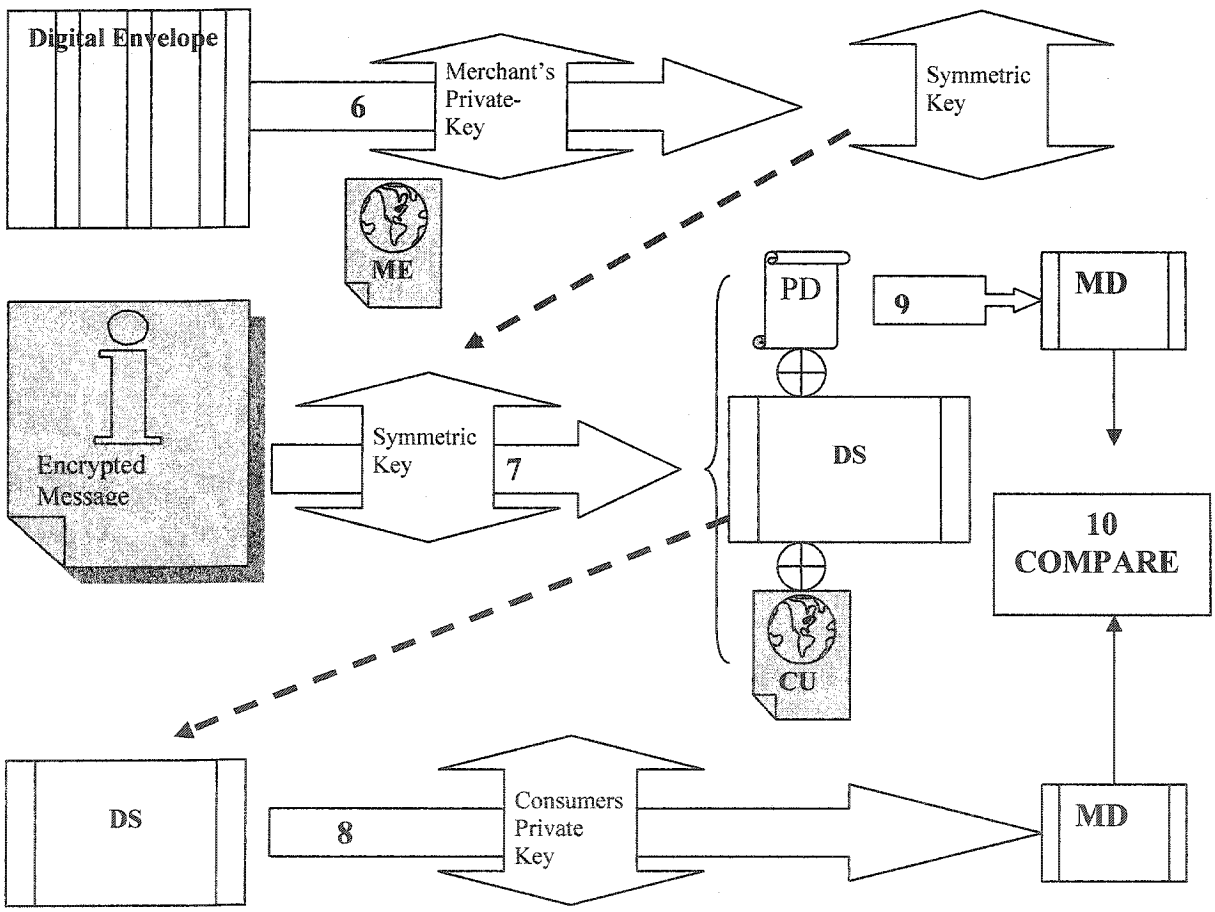



**Figure E.2 Decryption protocol, Based on SET Specification, Book 1: Business Description, version 1.0, May 31, 1997 [54].**

The operation of SET can be modeled as:

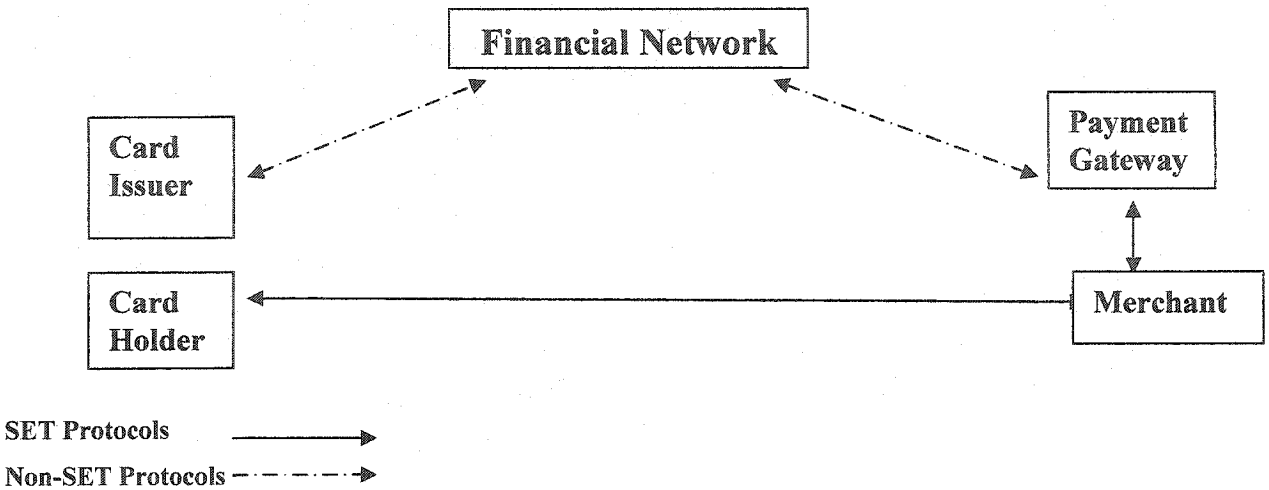



**Figure E.3 SET operational diagram.**

We can see from the diagram (figure E.3) that the SET protocol is employed among three parties: cardholder, merchant, and payment gateway. All other information flows are through a private network.

The SET protocol consists of request/response message pairs such as AuthReq/AuthRes, CertReq/CertRes, and PInitReq/PInitRes. Encryption is also performed on parts of certain messages. This feature enables the customer to hide certain data from non-intended viewers. For example, financial data about credit cards is hidden from the merchants, and the purchased product information is hidden from the acquirer.

It should be noted that the merchant never finds out the identity of the customers. After verifying the merchant signature and merchant's certificate, the customer prepares property description (which contains order information (OI) and payment instructions (PI)), OI, holds order information data and PI it holds cardholders data such as, purchase amount)). Cardholder software then encrypts PI with a randomly generated symmetric key (figure E.4). This key, along with the cardholder's account information, is then encrypted with the payment gateway public key, and then transferred to the merchant.

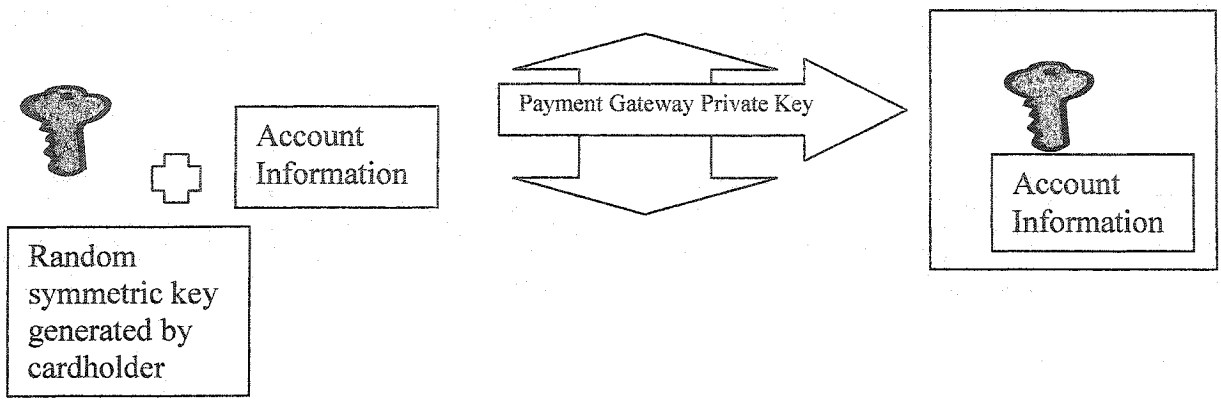



**Figure E.4 Consumers conceals his account information.**

The cardholder then transmits the encrypted information to the merchant. The account information is encrypted with gateway public key and therefore no one but the gateway is able to decrypt the information (figure E.5). Similarly, the merchant too encrypts his authorization request to the gateway and no one but the gateway can read the information.

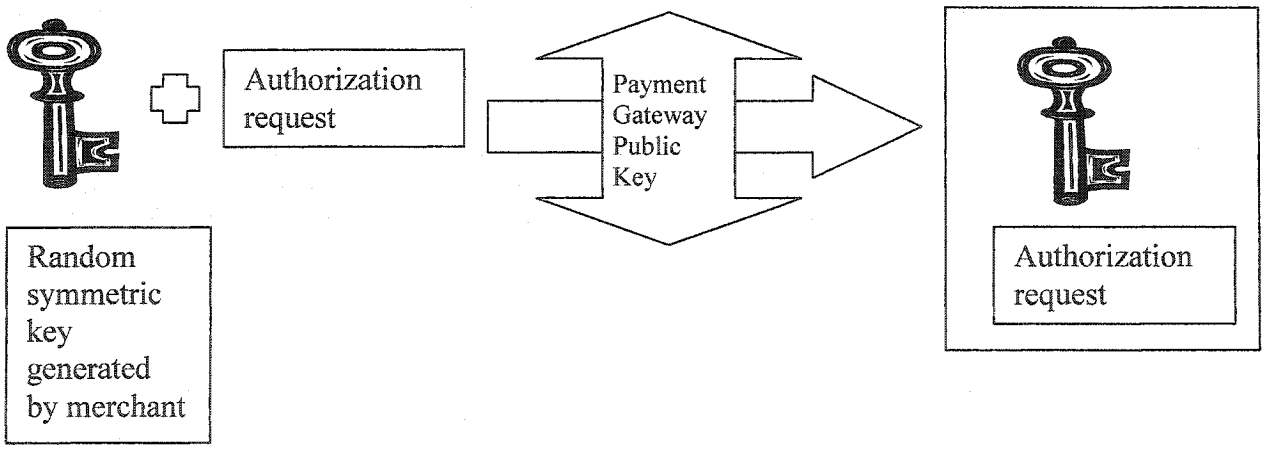



**Figure E.5 Merchants conceals their account information.**

The protocol can be briefly summarized as follows:

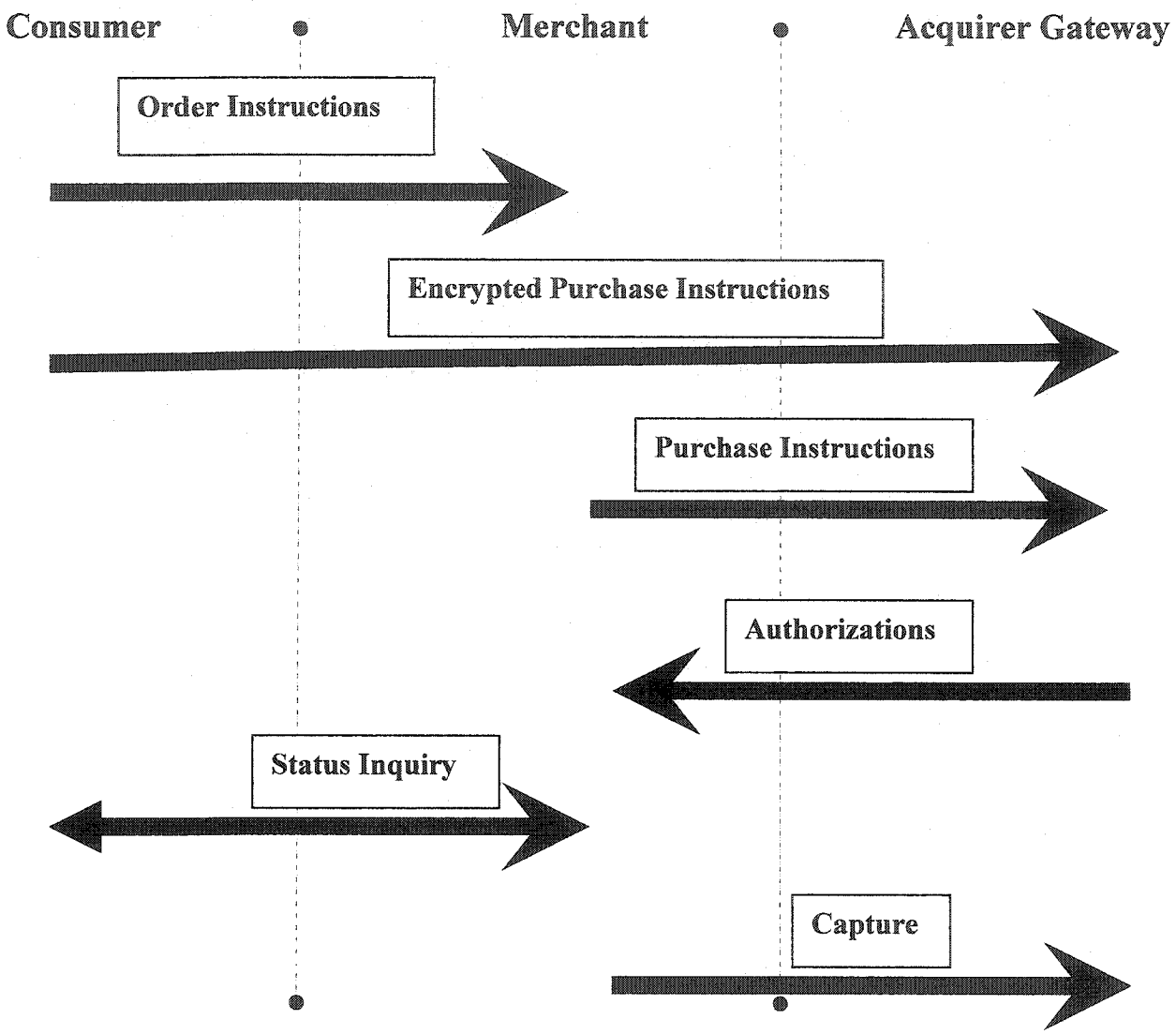



**Figure E.6 SET information flow.**

In the first phase, the card details are never shown to the merchant; rather all the information related to the card is encrypted and only the acquirer can decrypt that information. The merchant passes the purchase instructions to the gateway. The purchase instructions are cryptographically tied to the order instructions by dual signatures. Clients' digital signatures protect merchants from clients' repudiation. The acquirer can confirm that the cardholder and merchant agree on the purchase details. The complete SET protocol is more complicated than this. SET eliminates the need for an intermediary (all the authorization is done by the bank itself in real time) and that's why it has been so promoted. Also, it leverages the existing infrastructure.

However, it should be noted that SET is difficult to implement [12]. It is also very slow and resource-intensive. It needs users to have custom wallet software on the cardholder's PC, custom merchant software, and a special transaction processing software and hardware at the acquirer gateway.

### E.2.2 SSL

SSL [56] stands for Secure Socket Layer and was developed by Netscape. It is a basic encryption system. The software is designed to exist somewhat transparently just above TCP/IP (Transfer control protocol and Internet protocol layer). Any applications, say digital cash wallet software or smart card software, can initiate a TCP/IP connection using SSL and the software will ensure that the data travels encrypted.

Netscape released SSL 3.0 on November 18, 1996. SSL uses the public and private-key encryption from RSA, which also includes the use of a digital certificate. They use asymmetric algorithms in the handshake protocol to authenticate parties such as R.S.A, Diffie-Hellman, and fortezza. SSL can be implemented on any application as it lies on the transport layer, just above the TCP/IP layer.

SSL encapsulates the data transmitted between the client and the server in an SSL record. However, the SSL header is very small compared to an S-HTTP (secure-hyper text transfer protocol) header. SSL uses a handshake protocol in order to build up a secure channel for transmitting data. The client and the server have to agree on a cipher and a key.

The following is a pictorial representation of the handshake protocol:

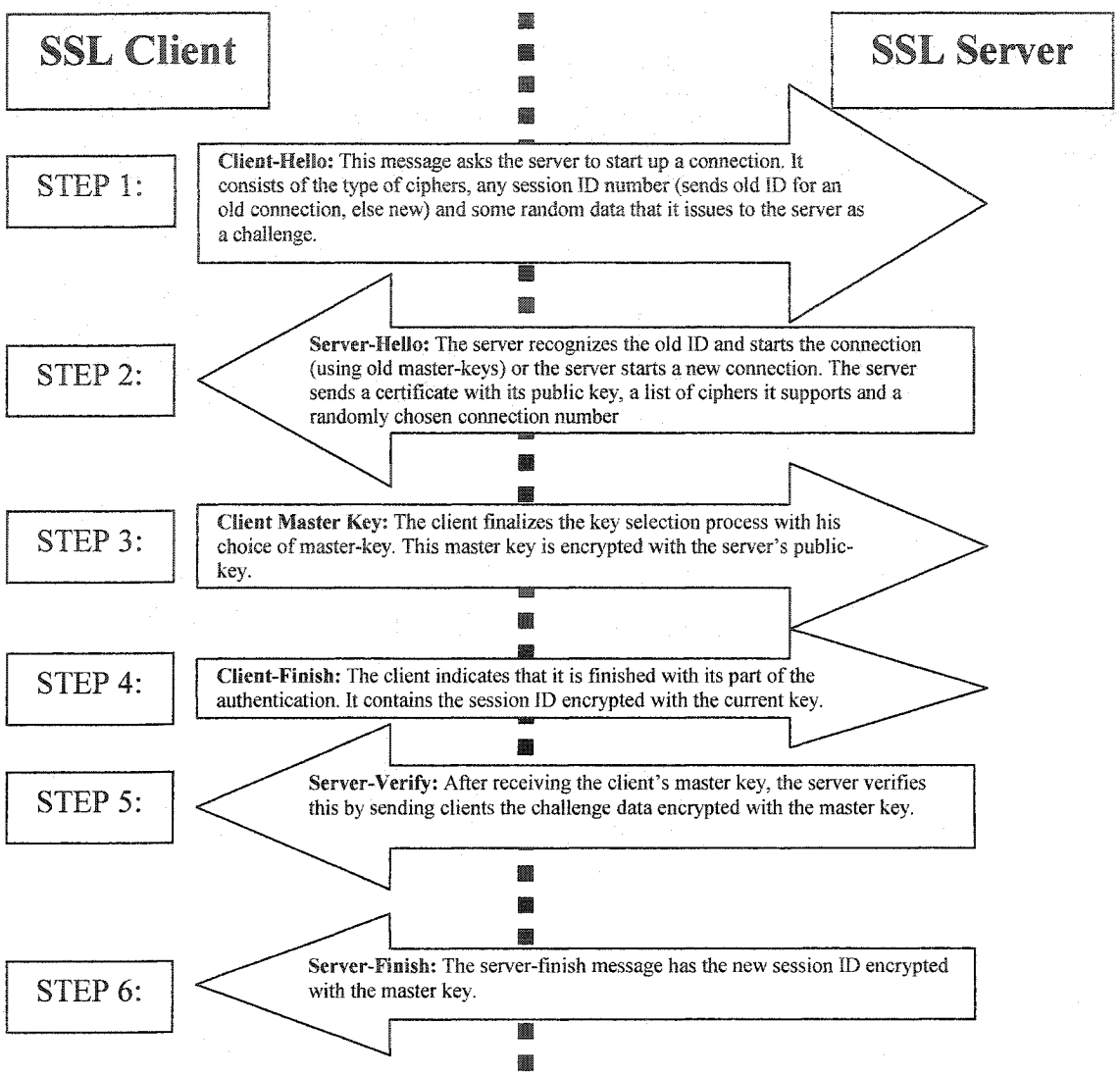



**Figure E.7 SSL operations, Based on SSL 3.0 Specification, November, 1996 [57].**

It should be noted that on the Step 3 (Client Master Key) in figure E.7, the key is sent in two portions: the clear portion and the secret portion. If the key for a cipher is "n" bits long, then the first "n-k" bits are shipped in the clear so anyone can read them and the other "k" bits are shipped encrypted with the server's public key. This was done to satisfy a U.S. export law, which says that RSA moduli larger than 512 bits may not be use'd for key exchange in software exported from the U.S. With this message, larger RSA keys may be used as signature-only certificates to sign temporary shorter RSA keys for key exchange.

HTTP(hyper text transfer protocol) clients often send messages beginning with GET to the HTTP server. A hacker could program his computer to generate all possible keys also known as plaintext attacks. If there were only 40-bits keys, it would be feasible to store this successfully for fast lookup. The software uses large key size (typically, 512 to 1024 bits) to reduces the possibility someone from creating a large dictionary and thus protecting itself against plaintext attacks.

Also, it should be noted that in the updated protocol released in 1996, some intermediate steps are:

1. Verification of server certificate just after the Server-Hello message.
   The certificate is generally X.509.v3 format.
2. Server key exchange message
   It is sent by the server if it has no certificate, has a certificate only used for signing (e.g., DSS [DSS] certificates, signing-only RSA [RSA] certificates), or fortezza/DMS key exchange is used.
3. Certificate request
   A non-anonymous server can optionally request a certificate from the client.
4. Server Hello done
   This message is sent by the server to indicate the end of the server hello and associated messages. After sending this message, the server will wait for a client response.
5. Client certificate
   This is the first message the client can send after receiving a server hello done message. This message is only sent if the server requests a certificate. If no suitable certificate is available, the client should send a no certificate alert instead. This error is only warning, but the server may respond with a fatal handshake failure alert if client authentication is required.

SSL also provides a mechanism for a client to use the older session keys by exchanging the older session ID. Both client and server maintain a cache of session identifiers which include encryption options received from the other system. SSL is a low-level protocol that negotiates a security level when a channel is opened and then becomes transparent to users.

In credit cards, issuers and acquirers sometimes choose to assign the processing of payment card transactions to the third party. The designated third party has a relationship with the acquirer's banks. Their essential role is to verify the transaction details received from the merchant, match them to those in the cardholder payment instructions, and then format, and send the authorization request to the issuer via the payment system. Merchants may opt for third-party credit card processors for the following reasons: if they sell a small number of products, live outside U.S., have little cash on hand, or want to get it done with little effort. Therefore, many startup merchants choose to outsource the payments to the third party. Some third-party credit card processors are Paypal, NoChex, iBill, and 2Checkout.

There are two types of processing while using credit cards. One is real-time Internet processing and the other is non-real-time Internet processing. In real-time processing, as soon as the customer clicks on the "Checkout" link in his shopping cart, he is transferred to a secure page where he types in his credit card information. In a matter of seconds, the cardholder will be notified if his transaction was approved or rejected. Real-time Internet processing providers automate the payment acceptance process. The third party processors do this in one of two ways. One is via a secure payment gateway (a third party who provides the connection to the processing banks via a land line) and the other is by their own proprietary secure payment gateway, and therefore does not require a third party. Some secure payment gateway providers are AuthorizeNet [58] and VeriSign [59] (formerly known as Signio). VeriSign introduced "Payflow Pro [60]", which enables the credit card numbers to go encrypted all the way to the processors.

The Payflow Pro (Signio) installs client software on the merchant's system, which establishes a secure connection, using SSL all the way to the transaction server, to securely exchange payment data between parties as shown in figure E.8. When the customer visits a Web site and enters his credit card number, it travels encrypted (via SSL) all the way to the Payflow pro client, which then securely passes the payment transaction data to VeriSign payment servers. No one (merchants or third party) can see the credit card numbers while in route.

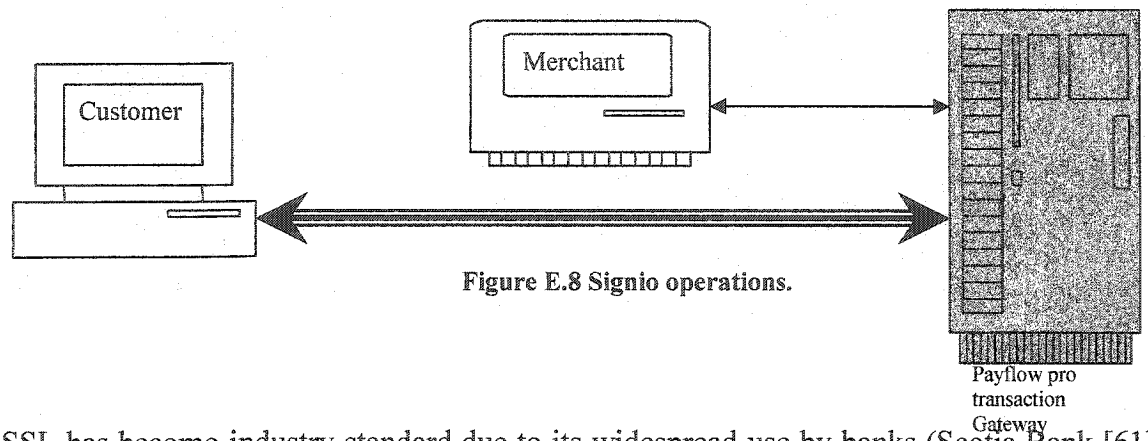



**Figure E.8 Signio operations.**

SSL has become industry standard due to its widespread use by banks (Scotia Bank [61], Royal Bank [62], and Bank of Montreal [63]) and online retailers (eBay and Amazon), who offer transactional services on the Internet. However, the banks need you to have an approved browser i.e., a browser that supports at least 128-bit encryption. Some companies that support electronic payment through credit cards (PayPal [64]) also support SSL protocol. SSL has been the first choice of Internet merchants, which accept credit cards as a form of payments.

The electronic commerce is mainly carried out by using either SSL or newly introduced SET protocol. Therefore, we will compare the e-commerce between SET and SSL.

## E.3 Comparative Evaluation

The comparisons between SET and SSL protocol for e-commerce transactions are as follows:

| **Criteria** | **SET** | **SSL v3.0** |
|---|---|---|
| Market release | YES ( April, 1997) | YES (December, 1995) |
| Encryption Supported | RSA,SHA,DSS,DES, 3DES | RSA, MD5, SHA, RC-4, CBC, DES, 3DES, DH, Fortezza |
| Need for Certification Authority | YES | YES |
| Ease of Use | Transparent to users (Must possess certificates in advance) | Transparent to users |
| Acceptability | NO (It is not widely popular) | YES |
| Customer Anonymity | NO | NO (The merchant possess client's information) |
| Monetary value Recovery | YES (Customer's liable to maximum of $50) | YES (Customer is liable to maximum of $50) |
| Peer-to-Peer payments | NO | NO |

**Table E.1 Comparative evaluation between SET and SSL v3.**

SSL's first version was released in July 1994. However, it was only in December 1994 that SSL v2.0 was shipped. Since then in 1995, Internet Engineering Task Force undertook its development and finally the currently used version (SSL v3.0) was released in December 1995. In February 1996, a Request for Comments (RFC# 1898, CyberCash Credit Card Protocol Version 0.8) was proposed by a networking group.

Both SET and SSL are highly secure. They use the latest cipher in the market. They use RSA with keys greater than 128-bit and latest symmetric key encryption. As can be seen from the table, SSL v3.0 supports many more ciphers than SET. One of the reasons being is that the SSL was designed to negotiate between the client and server to come up with the best possible choice of ciphers. SSL is based on mutual authentication of merchant and customer using the certificate at the time of communication; whereas SET is based on trusted third-party authentication and no dialogue takes place between client and server. Also, it should be noted that before the connection is established, during negotiation stage in SSL, the clients and server come across a range of options of ciphers. As defined in cipher suite in SSL specification [57] (on page 40), the following are the range of cipher options supported in SSL; RSA with MD5, RSA with SHA, RSA with RC4 -40-MD5, RSA with RC4-128, RSA with RC4-128-SHA, RSA with RC4-CBC-40-MD5, RSA with IDEA-CBC-SHA, RSA with DES-CBC-SHA and RSA with 3DES-EDE-CBC-SHA. It should be noted that all the ciphers with 40-bit encryption are meant for export. As per U.S laws, the encryption greater than 40-bit key size could not be exported. Also, there is a separate suite of cipher definitions that are used for server-authentication.

Both protocols require the use of a certification authority, as they involve exchanging certificates certifying their authenticity. The public keys certifying the identity are very big, typically 1,024 bits to 2,048 bits long. This has been done to make breaking the key very difficult. The key size is expected to increase with the increase in computation power. SSL and SET are transparent to users and they are programmed as such to verify the public key and certificates and refuse access to unauthorized users.

SSL has been a huge success and is considered by many to be the *de facto* standard for Internet transactions. Most of the Internet retailers and banks use it. By contrast, SET has not been widely popular.

Customers are not anonymous when they use SSL. It is the responsibility of the merchant to pass on the information further to the acquirer. However, the customer remains anonymous in SET as the credit card information and other details authenticating him go directly to the acquirer. The acquirer simply authorizes the transaction to the merchant and thus, the merchant accepts the dealings.

Both the protocols do not permit peer-to-peer as they have been designed for payment through cards. They restrict themselves to transactions involving to merchants online. However, in the future it might be possible to pay anyone.

## E.4 Strengths and weaknesses of SSL

| | Consumer | Merchant |
|---|---|---|
| Strengths | Transparent to consumers, high end security, guaranteed fraud protection | Quick hassle-free transaction, store transaction details, option of outsourcing processing, simple to deploy. |
| Weaknesses | Need to have valid certificate, latest security software, update certificate revocation list, not anonymous, need to give credit card number on Internet. | Expensive shipping cost in case of fraud, need to have certificate, update certificate lists, and need to maintain a server with database. |

**Table E.2 Strengths and weaknesses of SSL.**

## E.5 Strengths and weaknesses of SET

| | Consumer | Merchant |
|---|---|---|
| Strength | Transparent, secure, quick, no information is given to merchant and maintains privacy, stronger fraud protection. | Quick hassle-free transaction, lowers the risk of credit card being stolen, accepts cards from multiple issuers |
| Weakness | Need to have valid certificate, robust and resource intensive protocol, latest security software, update certificate revocation list | No consumer information or details are stored, shipping cost in case of fraud, need to have certificate, update certificate lists, hard to implement. |

**Table E.3 Strengths and weaknesses of SET.**

# Appendix F

# Other forms of online payment

Many new online payment mechanisms have been launched. In this chapter we will discuss, "online banking using a reader, e-mail money transfer and charging to one's phone bill." We will analyze them and highlight their strength and weaknesses.

## F.1 Online banking

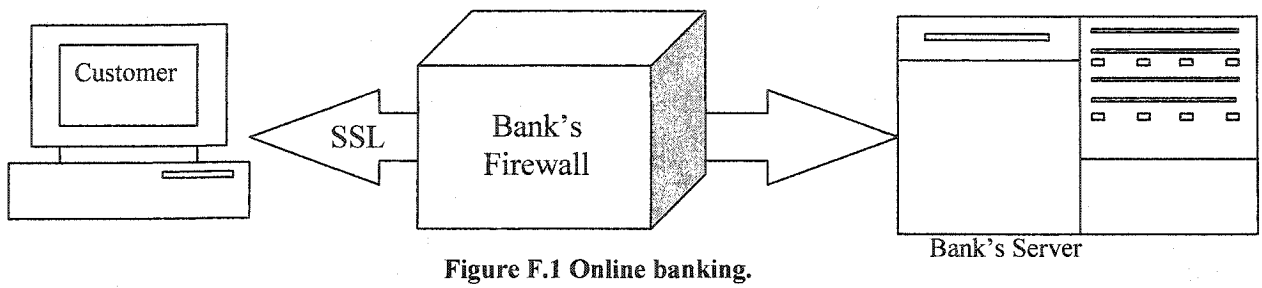



**Figure F.1 Online banking.**

Online banking allows customers to access their accounts conveniently through the World-Wide Web. Major Banks around the globe offer this feature today, which has become very popular for the payment of bills and for keeping one's peace of mind. The customers are allowed full access to view their accounts, their balances, and transaction log (both current and history). They can also pay their bills online for various services and utilities. Some advanced feature also includes buying and selling stocks and other investment services.

First, online banks started appearing in the U.S. "Wells Fargo" (a leading bank of North America) introduced it in 1990, and since then, many banks have integrated their system online. Many new services are being added to the online banking every year, giving consumers more control of their accounts and finances. Consumers find online banking a very attractive option because it offers lot of convenience. The consumers can access the online bank twenty-fours hours a day and seven days a week (Unless the system is down because of the network). Also, consumers are allowed to use some of the basic features like paying bills, transferring money, e-mailing money, investing in stocks, and managing investments. Along with convenience, online banks also offer ubiquity. They allow access to the personal bank accounts and other services,

from anywhere where there is a coverage, using wireless devices such as laptop computers, PDAs (new PDA devices with WAP browser), and mobile phones that support Internet access.

Some payment gateways have come up with certain devices such as card reader, infra-card reader, which can read an A.T.M card securely through a computer and therefore conduct a transaction.

The banks rely on highly secure networks to provide their services. Their system is protected by firewall software to avoid attacks (figure F.1). They also have constant monitoring to prevent any unruly attacks from inside. They use SSL with very large size keys (1,024) for the certificates to identify the users. They would not allow access without SSL and therefore the browsers have to be updated to support 128-bit encryption. Along with SSL-only access, the banks also have session timeouts if no activity is reported for a period. They update their security software regularly and update all the certificates at regular intervals.

Along with the banks, the users are also expected to protect their passwords and keep their systems updated with the latest software. They are expected to have antivirus software and are advised to act with caution and responsibly while online transaction.

An example of online banking is "ECashNetwork" [65], which allows consumers to use their ATM cards with a PIN, using the reader to accept transactions. Such payments are relatively new and will take a while before they are fully accepted in the market. They use propriety technology to secure the communication link. However, the consumer has to spend some amount to buy a reader if using an ATM card. The operations of "ECashNetwork" are briefly shown in figure F.2.

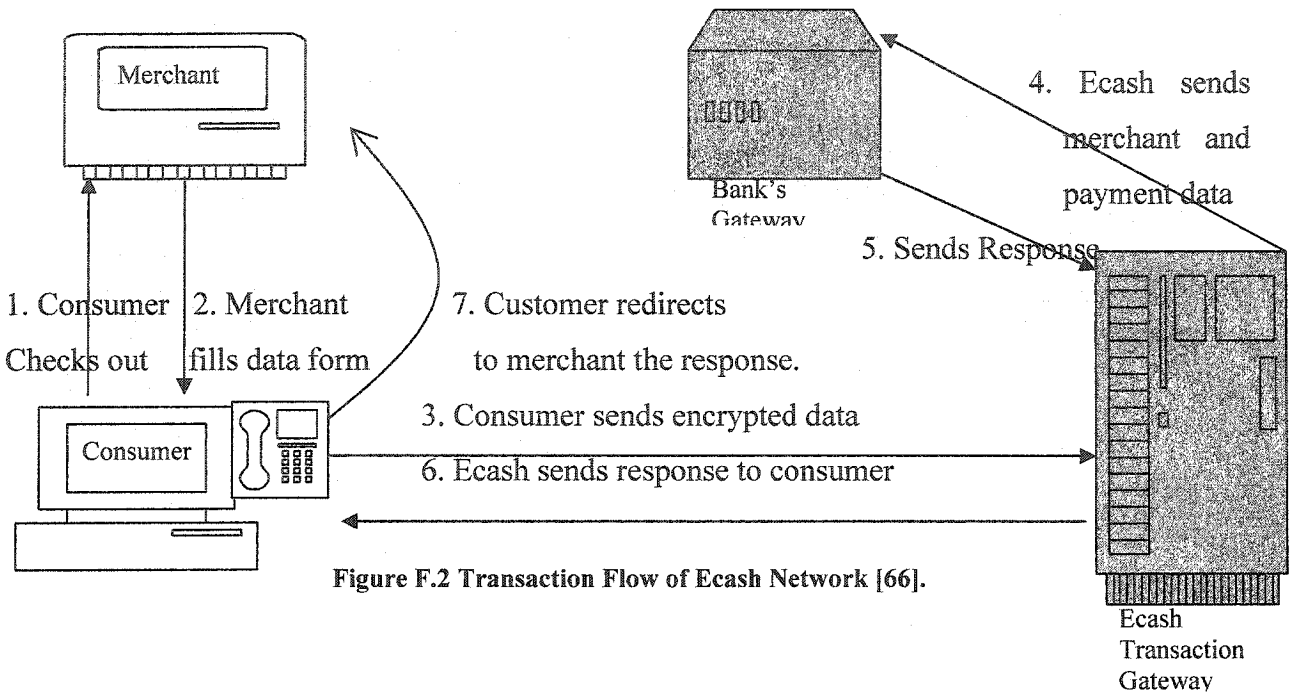



**Figure F.2 Transaction Flow of Ecash Network [66].**

The transaction starts when the customer checks out and the merchant sends the customer appropriate data (Merchant ID, order number, amount, etc.) encrypted with his public key along with his certificate issued by the certified authority. After obtaining all the appropriate information, the customer swipes his card on the terminal, enters his PIN, and sends all the information to the payment gateway. The payment gateway server checks the authenticity of the merchant and its order and sends all the information to the bank for approval. The bank sends their approval or rejection to the payment gateway, the reply is further redirected to the customer, and the merchant with it's a message digest (for verification of validity).

The users have to buy the P.O.S device, which costs U.S $59.and 95 can be fitted into the USB port of his computer.

## F.2 E-mail Money Transfer

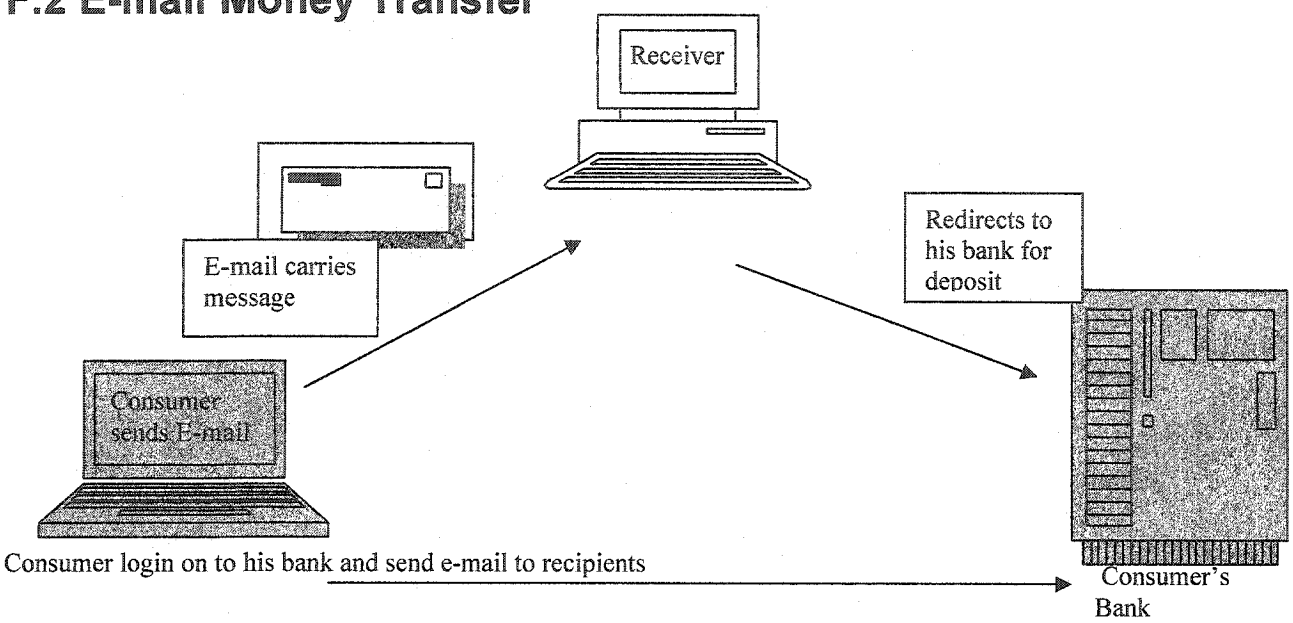



**Figure F.3 E-mail money transfers.**

Another example is Certapay [67]. Certapay allows money to be transferred by e-mail. It is being offered by all major banks in Canada. The consumers go to their respective bank Web sites and write off an e-mail to respective merchant. They add a secret question and its answer (whose answer has been mailed to the merchant earlier). Now, the bank sends an e-mail to the merchant with a request for the answer for the secret question. The bank ensures security by asking the merchant to click on a specific link and the merchant is directed to a secure Web site where he is supposed to answer the question as clarified in figure F.3. If the answer matches the question then, the bank asks the merchant the account where he wants the money to be deposited. The money transfer is fast, convenient, instant, and secure. Anyone who has an e-mail account can be paid the money. However, one drawback of the system is that the fee involved in the transaction is typically CAD $1.50 which is expensive for a small value transaction. Also, the maximum amount that can be sent using this system is limited to CAD $1,000. However, with the advantage of being e-mail-based, the Certapay can be used to pay for services, send money to friends and family, and can be used for payment on Internet auctions. It should be noted that the e-mail money transfer also uses SSL for secure transfer. When merchants receive the e-mail, they are linked to a SSL protected server.

## F.3 Charging to one's phone bill

Some payment systems provide the provision to buy digital goods or merchandise over the Internet and charge those purchases to one's phone bill. One such system is offered by eCharge [68]. They claim to be more secure as the user never has to enter his credit card information online. They are billed on a monthly basis on the phone bill. It should be noted that no information is passed to the merchant, thus ensuring the privacy of the customers.

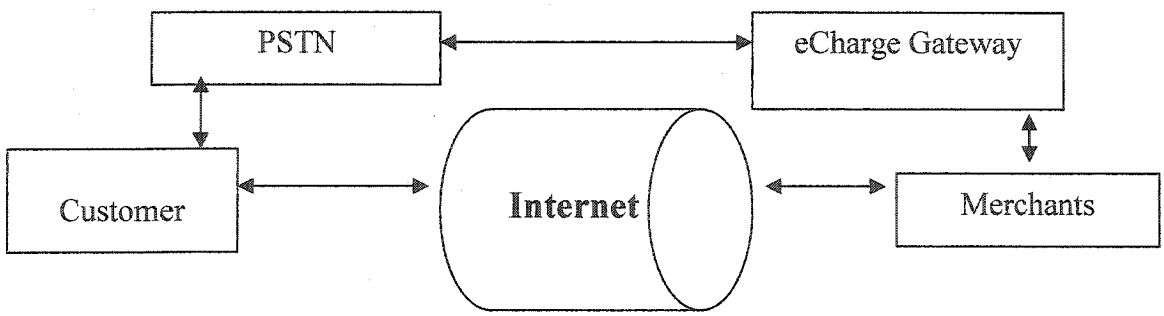



**Figure F.4 Charging to one's phone bill.**

When the customer is ready to buy, he chooses his method of payment. The computer automatically downloads the software to dial the client software. This is special software that allows the customer to connect to the payment gateway securely and reliably. Once the software is successfully downloaded and installed, it automatically dials for gateway access (using the existing phone line). Once connected, it processes the payment and shows the customer what he is paying, for confirmation. The software also captures the customer's telephone number in the process and shows the customer the total charges he will be billed for the item in his telephone bill. This bill includes the service charge that might be incurred, and he is given the option to purchase the item right away or some other time. Based on the user response, the software goes ahead, dials the number, and completes the transaction process. The software informs the merchant upon the successful completion of the transaction process and the merchant begins the process of shipping the goods. The whole process is very systematic and no personal information is sent to the merchant, and the transaction is carried out in a very secure and reliable manner. The mechanism is shown in figure F.4.

The customer needs to have a computer with a dial-up modem and a phone line and the telephone number is captured when the payment is being made, which makes it very difficult for

someone else to hack the system and commit fraud. Also, the transaction goes through a phone line that is perceived to be more secure than Internet (HTTP). They use SSL along with digital signatures to secure the communication.

## F.4 Comparative Evaluation

Now we will compare between the three types of online payment as mentioned previously:

| **Criteria** | **Online Banking using Reader** | **E-Mail Money Transfer** | **Charging to one's phone Bill** |
|---|---|---|---|
| Market release | YES | YES | YES |
| Security | Digital signatures, SHA, gateway deletes all sensitive data | SSL, Secret Question | SSL, Pass-Phrase, Digital Signatures |
| Need for Certification Authority | YES | YES | YES |
| Ease of Use | PIN entry, Need to have ATM Card (and Reader), Certificate, Updated Software | Check E-mail once within 24 hour, Need to send answer to secret question beforehand, Need bank Account for accessing funds | Transparent to users, No need to enter any Numbers |
| Acceptability | Not Available | Not Available | Not Available |
| Customer Anonymity | NO | YES(anonymous to merchant) | NO |
| Monetary value Recover if Fraud | NO | NO | NO |
| Peer-Peer pay | NO | YES (must have account with bank) | NO |

**Table F.1Comparative evaluation of online banking using a reader, e-mail money transfer and charging to one's phone.**

All the systems have been released in the market. Certapay is the newest one, having been released in 2000; eCharge has been there since 1997.

ECashNetworks offers security to merchants by digitally signing the order information to avoid any tampering using a merchant's public key issued by a certified certificate authority. The customer PIN is encrypted in the local machine and travels encrypted to the bank. A message digest is found, and the bank responds and sends it back to the merchant and customer for verification of authenticity. E-mail money transfers involve sending secret questions and

answers. The sender must notify the receiving party of the answer to the secret question beforehand. The sender has to log in to the bank's Web site to send the e-mail. Therefore, he uses SSL (the same as the one used for online banking). The receiver receives an e-mail; he is directed by a link to the bank's secure server (SSL login). The receiver has to log in to a secure environment and accept the fund transfer. He also has to answer the appropriate question correctly. The systems employing charges to phone bills use SSL with a pass-phrase. The identity of each applicant is thoroughly verified before being allowed to open an account. It should be noted that it is entirely the user's responsibility to protect his computer; otherwise anyone online can make a purchase using the customer's computer.

All the above-mentioned systems, "online banking using devices," "e-mail" money transfer, and "eCharge," need a certification authority for the surety and verification of the public keys. Companies like "eCharge" download software into the user machine, which finds out the telephone number the computer is connected to.

eCharge is definitely easier to use than the other two systems as the user does not have to enter a PIN or number of any sort to make a purchase. The software detects the phone number automatically. Purchasing items are just a mouse click away. However, in the other system using online banking or even those using credit cards, the customers have to enter their card number manually (unless using wallet software).

The number of online bank and e-mail money transfer users is increasing. From the U.S government census report [6] Statistical Abstract, published in 2004, the banking, financial and insurance section projects growth in the number of ATM and other cards. We cannot find any direct data on e-mail money transfers or charges on phone. Presumably more and more people will start using it for its convenience.

The customer needs to have an account with the bank in order to use online banking. Upon choosing the method of payment, they are directed to their respective payment gateway where the payment is verified and authenticated. When the authorization response has been made, the gateway sends this information back to the customer and merchant. In the whole process, the

merchant does not receive any client personal or financial information. Therefore, the customer remains anonymous. While in e-mailing money transfer both customer and the merchant need to have accounts with their respective banks. An e-mail is sent to the merchant on behalf of the customer by the bank with the secret question. Upon the correct answering of the question, the merchant is credited with the given amount. However, the merchant never finds out the customer's identity; therefore, the customer remains anonymous. In charges by phone, the software records the phone number of the customer and the payment gateway approves the transaction. The merchant receives a go-ahead of the transaction from the gateway. He does not receive any financial or personal information; therefore, the customer remains anonymous to him.

None of the above-mentioned systems are protected by federal laws like that for credit card which guarantees the consumer a maximum liability of $50. They involve all the security features; however, in case of any fraud, it is the responsibility of the customer or the merchant.

ECashNetwork does not allow peer-to-peer payment. It is only meant for business to consumer or vice versa. With e-mail money transfers, we can pay anyone with an account at a bank which accepts "Certapay" and has an e-mail address. It is the user's responsibility to exchange secret questions and answers from other users. This can easily be done using phone, e-mail, or letters. Charging to one's phone is only available for buying or selling through an online merchant.

## F.5 Strengths and weaknesses of "online banking using device"

| | Consumer | Merchant |
|---|---|---|
| Strengths | Added convenience, added security, added consumer confidence, anonymous | Added security, added consumer confidence, accepts multiple cards, instant fund and reduces consumer fraud |
| Weaknesses | Purchase a card reader, no compensation against fraud. | Loss of consumer information, need to get certificate from valid certification authority |

**Table F.2 Strengths and weaknesses of online banking using a card reader.**

## F.6 Strengths and weaknesses of "e-mail money transfer"

| | Consumer | Merchant |
|---|---|---|
| Strengths | Added convenience, added security, added consumer confidence, anonymous, pay to anyone. | More consumers, can be ubiquitous, immediate access to funds |
| Weaknesses | High transaction fee, no compensation against fraud | Needs to have an account with the bank accepting transfer, frequent checking of e-mails |

**Table F.3 Strengths and weaknesses of e-mail money transfer.**

## F.7 Strengths and weaknesses of "charge to phone bill"

| | Consumer | Merchant |
|---|---|---|
| Strengths | No need to swipe any card, added convenience, no need to enter any number or PIN, added security, enables micro-payments | Lower fees, broader consumer base, more security |
| Weaknesses | No anonymity, need for a computer with modem, need to have land phone line, no fraud protection | No compensation against fraud, only for Internet purchases |

**Table F.4 Strengths and weaknesses of charging to one's phone bill.**

# Appendix G

## Mobile Commerce

Mobile commerce can be defined as using a mobile phone or any other mobile device (viz. PDAs) used for commercial applications. Commercial applications include advertising, buying and selling of merchandise or stocks, using the handheld device to pay bills, sending e-mails, buying ringing tones, games, and horoscopes, travel booking, and entertainment.

Mobile commerce gives the user unprecedented convenience. The user can buy stock at the last minute or keep up-to date with sports scores, weather reports, traffic jams, travel itineraries, nearby restaurants, and mobile banking. Some merchants have shown an interest in a system where an SMS (simple message service or text messaging) is forwarded to a group of users about special deals. It is also an attractive option for location-based services and advertising. The consumers benefit with more information on their end. It is also a source of ubiquitous and customized information for them.

However as convenient and attractive as it sounds, mobile phones has not been hugely successful in attracting customers for businesses. The reasons lie in the fact that most of the predictions about the popularity of mobile commerce were based on predictions about mobile phones themselves.

In spite of being the world's largest wireless voice market, the U.S has relatively low penetration of cell phones. Moreover, consumers need to grasp the idea first. If we follow the example of e-mail: it was available for years, but consumers didn't begin using it until they became comfortable with it. As of March 2002, only 1.4% (Jupiter consumer survey) of consumers who own Internet-ready wireless devices had made a purchase using the capabilities on their cell phones or Personal digital assistance (PDA) (Jupiter consumer survey reports) in North America. The industry officials assumed that if a person has shopped the Web from his home computer, he would easily switch over to buying things from a mobile telephone or device. Industry officials ignored the fact that consumers need to accept ideas first.

Some other reasons might be the operation of mobile networks themselves, i.e., slow wireless connection speed, small browsers, security concerns, and slow processing power of the devices. With the advent of 3G wireless networks and the introduction of PDA, wireless networks are said to have revived and we are looking at brighter prospects. The spectrum in use with 3G is around 2.4 GHz, and wireless networks have more bandwidth available for use. This has opened a plethora of options for what we can do with wireless networks.

According to Ghosh and Swaminatha (2001), major applications include Web access for information services such as weather reports, sports scores, etc. However, the Yankee Group (2000a) discovered limited consumer interest in such applications, with only 19% of European mobile users interested in information services. Kannan et al. (2001) argue that the most significant possibilities in m-commerce lie in the marketing of services such as interactive games, gambling, travel bookings, banking, and applications related to the financial industry. In 2000, online services were offered by 94% of all banks in Europe (Muller-Versee 2000), and wireless technologies are expected to expand the benefits offered by online banking. Surveys show that 29% of the Europeans are either interested or definitely interested in mobile banking (Yankee Group 2000a). According to Varshney (2001), mobile financial applications are likely to be one of the most important components of m-commerce. A mobile device could turn into a business, replacing bank, ATM, and credit cards, thus allowing for value-added services such as micro payments for purchases at vending machines and payments in shops (Varshney and Vetter 2001). According to Senn (2000), the highest m-commerce transaction volume will probably occur in micro-transactions. However, more advanced financial activities such as loan negotiations and sending notifications of claims to insurance companies could also become feasible through mobile devices.

## G.1 Mobile Browsers

A Web browser is the software which allows us to surf Web pages while connected to the World-Wide Web. Many competing mobile browsers are available today (Blazer, PalmScape, and Netfront). The browsers used are of two types. The first are "online browsers" which allow

users to actively visit Web pages using active Internet connections; the other type is "offline browsers," which store the Web pages during synchronization for later viewing. For e-commerce, we most certainly will restrict ourselves to the discussion of "online browsers." Many browsers are available in the market. Some of the new ones have support for regular HTML pages, WAP (WML (wireless markup language) and XHTMLMP (XHTML mobile profiles) for WAP v2), and cHTML sites. The Web browsers available for wireless devices can be classified in two types: ones that use a proxy server while connecting to the Web and ones that establish a direct connection (like a regular PC). The proxy server does the work of retrieving the selected page on behalf of the user and formats it to suit the user's device (i.e., takes into account the small screen and limited memory and speed). The browsers that connect through a proxy are faster than those that don't. However, the downside is they don't allow all the applications to work on the device as they strip out unnecessary and unsupported content (the user does not have a say). Therefore, this trade-off is the essential point of the consumer's decision to adapt the browser and it depends on each individual's view. However, most browsers are capable of making secure connections.

## G.2 WAP and Security

Wireless transport layer security (WTLS) [69] is the security layer of Wireless Access Protocol (WAP), which is the most widely used and the standard for providing security, privacy, data integrity, and authentication for applications in mobile phones and other small wireless terminals. Before examining how WTLS works, we should first look at the WAP network architecture. The WAP-enabled phone or PDA communicates directly with a gateway. A gateway is a server that decompresses Wireless Markup Language (WML, a subset of XML) and translates it into HTTP. The request then follows, like ordinary Internet packets. Implementing WTLS makes WAP secure by encrypting the communication between the gateway and the device (phone or a PDA). When the user enters any sensitive information, it is encrypted using WTLS between the devices to the gateway. At the gateway, the content is decrypted and re-encrypted using SSL to the appropriate server.

WTLS bears a close resemblance to SSL. However, some changes were made to suit the wireless connection requirements. The WTLS was designed to accommodate for long round trip or delays in the wireless networks. Also, there was a consideration for limited processing power and memory of the devices. Along with all these facts the designers also took into account U.S. export restrictions on cryptography in force at that time. Some newer versions of the WAP specification address the shortcomings in WTLS. Other flaws that were brought to light by Markku-juhani Saarinen of the University Of Jyvaskyla, Finland, include plain-text data recovery, the datagram truncation attacks, the message forgery attack, and the exportable key-search shortcut [70]. Also, m-commerce does not yet factor in support for security mechanisms such as digital certificates, though work has begun in this field, introduced by Entrust [71] on a trial basis. Finally, there could be a compromise on the gateway itself where the data is decrypted and re-encrypted.

Much work has to be done before the use of m-commerce becomes wide spread. Consumer confidence in using the system has to be raised by addressing security and privacy concerns. The loopholes in the system has to be addressed (the point where an encrypted data is decrypted and encrypted again at the gateway). Some other issues include clumsy interfaces, cumbersome applications, low speed, and expensive services.

## G.3 PDA (Personal Digital Assistants)

PDAs represent a new era of mini-devices. They are also commonly referred to as hand-helds. One of the first PDAs to be introduced was by Sharp Corporation, Japan in the early 90s.

PDAs can be held in the hand and they do not need a keyboard for input; rather they come with a thumb pad or handwriting recognition software. PDAs allow consumers to organize and write memos. Some new PDAs have the capability to connect to the Internet directly. However, Internet-enabled products, needs a browser to view the contents of the web page. We will analyze widely available internet browsers for PDAs (table G.1).

PDAs offer consumers ubiquity and convenience. Users do not have to wait in line for movie tickets or sit in front of a PC at home; they can choose the movie on the way and buy tickets while driving there.

The browsers used in PDAs are "online browsers" which allow users to surf the Web. PalmOne latest product "Treo 600," uses the "Blazer Web browser." Sony, in products such as "PEG-UX50," "PEG-TH55" and "PEG-TJ37" uses the "Netfront." Casio, with its product "Cassiopeia Pocket PC 2002, E-200," uses the "Pocket Internet Explorer." Similarly, BlackBerry includes a browser, which can support end-to-end HTTPS connectivity [72].

Following is a comparison chart between the browsers used in various devices:

| | NetFront v3.0 | Blazer | Pocket IE |
|---|---|---|---|
| Proxy Used | NO | YES | YES |
| Java Enabled | YES | NO | NO |
| 128 bit Encryption | YES | YES | YES |
| WAP Supported | YES | YES | YES |
| HTML Supported | YES | YES | YES |
| cHTML Supported | YES | YES | YES |
| Images and Sounds | YES | Images YES, Sound NO | YES |
| Frames | YES | YES | NO |
| File Download | YES | NO | YES |

**Table G.1 Comparison between mobile browsers.**

## G.4 Mobile Phones

Mobile phones have been increasing in demand ever since their introduction. They are also popularly called cell phones. This is because the system uses many base stations to divide a service area into multiple "cells." Cellular calls are transferred from base station to base station as a user travels from cell to cell. Bell Labs introduced the idea of cellular phones in 1947 by the introduction of police car phone technology. However, it was not until the late 80s that cell phone demand really picked up.

The cellular network system facilitates mobility in communication. Systems achieve mobility by transmitting data via radio waves. Some of the most commonly used mobile communication systems are paging, cellular radio networks, personal handy phones, and mobile radio.

Cellular radio systems, implemented for the first time in advanced mobile phone systems (AMPS), support more users by allowing the reuse of frequencies. AMPS is an analog system and is frequently referred to as 1 G (first generation wireless networks), based on the idea of cells. It employed Frequency Division Multiplexing (FDM). Another mobile network system uses Time Division Multiple Access (TDMA), a method by which each conversation only uses a frequency for part of the time (also called D-AMPS). The TDMA system works by dividing a frequency into a number of time slots, each of which corresponds to one communication channel. A cell phone transmits and receives in only one slot, remaining silent until its turn comes around again. The second-generation (2G) systems are digital. They employ Code Division Multiplexing (CDMA), a system that enables many users to share the same frequency band at the same time. Each signal is encoded differently so that a receiver with the same code can understand it. Now with the evolving technology, different countries have adopted different standards. In the U.S. alone, two standards are used: IS-95 (CDMA) and IS-136 (D-AMPS). Europe consolidated to one system called the Global System for Mobile Communication (GSM). GSM is by far the most widely used standard [73]. Japan uses a system called Personal Digital Cellular (PDC) which is based on TDMA. The maximum data transmission rate for 2G networks was 9.6 Kbits/sec to 14.4 Kbits/sec; enhanced features included caller-ID and text-based messaging.

The next network to emerge was named 2.5G, which is still not available everywhere; it is essentially General Packet Radio Service (GPRS) packet overlays on 2G networks. Besides enhancing GSM and TDMA networks by adding packet-based networks, GPRS also increases their data rates (64 -144 Kbits/sec). The third-generation (3G) of wireless networks is the latest one to emerge and it not only offers a breakthrough in bandwidth but also the way we use wireless systems. 3G uses packet-switched connections and Internet Protocol; this means the terminal is virtually always connected to the network. Moreover, the higher bandwidth allows for more new services, such as video conferencing, mobile online shopping, positioning, and multi-

media streaming. 3G boasts data rates up to 384 Kbits/sec for moving users and up to 2 Megabits/sec for stationary users.

Mobile phones are also sometimes seen as items of novelty. However, with the introduction of m-commerce, recently it has not only become a necessity but also an objective convenience. Most phones offer features like text messaging, SMS, Internet browsers, digital cameras, MP3 players, and voice recorders.

Mobile phones offer a number of challenges because of their limited memory, storage, and processing power. Internet connections in mobile phones use non-trusted, public networks. Also, mobile phones frequently change locations, sometimes even from one type of network to another. However, with the growing number of users, the phone companies are trying to introduce more services to consumers. Such services include data exchange, Internet capability, and video messaging. So far, consumer response to these features has been minor. Consumers are definitely concerned about security in phones. Several companies have been working in the field of security and so far the most promising feature is the deployment of WTLS in mobile phones.

WAP v1 has already been described as the standard in wireless data communication and thus, WTLS is the natural choice for many developers and service providers. WTLS, like SSL, is designed to lie just above the transport protocol layer [74]. The WTLS layer is modular and it depends on the required security level of the given application as to whether it is used or not. WTLS provides the upper-level layer of WAP with a secure transport service interface that preserves the transport service interface below it. In addition, WTLS provides an interface for managing secure connections. WTLS incorporates new features such as datagram support, optimized handshake, and dynamic key refreshing. The WTLS protocol is optimized for low-bandwidth bearer networks with relatively long latency (cycle time). The latest version of WAP v2, released in August 2002, is based on TCP/IP protocols, and thus does not need a proxy to go to the wired network. The use of the proxy is limited to location-based services and push functionality. It makes use of XHTML mobile profiles (XHTMLMP) instead of WML.

Going by the statistics, mobile phones are more popular in Europe and some pockets of Asia than in North America. One of the main reasons for lower popularity of mobile phones in North America is the presence of a large and extensive wired phone network. The penetration rate or share of households with cell phones in the U.S. in use is 40%. By contrast, in Europe and Asia penetration rates exceed 70% in some countries, according to Jupiter. Finland and Taiwan have penetration rates of 72% (Jupiter consumer survey).

However, the potential for wireless technology and accompanying applications continues worldwide. Industry experts predict there will be:

- 177 million subscribers to mobile services by 2005 (Forrester Research) and
  11 million U.S cell phones users connected to the Web by 2005 (Forrester Research).

With the popularity of mobile-commerce, a new billing approach emerged called "content based" billing in which the usage charge is based on packet data volume instead of duration of call.

NTT DoCoMo is a leading communications company from Japan and it is the first company to introduce 3G service; it currently boasts the highest number of subscribers in Japan [75]. They have been forerunners in promoting i-mode service. The "i" in i-mode actually stands for information but it is also a play on the Japanese word for "anywhere." To create a page for i-mode, developers have to employ a special subset of HTML known as compact HTML or cHTML. About 70,000 content providers currently support it. We will compare these two modes of service in table G.2.

| | WAP | i-mode |
|---|---|---|
| Based on | Wireless Markup Language | Compact HTML |
| Security Layer | Wireless Transport Layer Security (WTLS) | SSL |
| Acceptability | Widely accepted in many countries all around the world | Only in Japan, Taiwan and a few countries in Europe (Spain, Germany, France, Italy, Netherlands, Belgium [76]) |
| Implementation | Circuit-Switched networks and Packet-Switched network where available | Mostly on Packet-Switched networks |
| Billing Approach | Connection-based and Content-based [77] | Content-based |
| Java Support | YES [78] | YES[79] |
| Platform | Open forum and standards [74] | Proprietary |
| Content Control | NO | YES |

**Table G.2 Comparison between WAP and i-mode.**

With the above evaluation we can conclude that the main difference between i-mode and WAP is the billing approach. We will compare the prevalent billing approaches between the two modes in the table G.3.

| | Content Based (i-mode) | Flat Rate (Connection-based) |
|---|---|---|
| Content Control | YES<br>All content must be authorized by NTT DoCoMo. All content is continually updated, kept as comprehensive as possible, and designed for maximum clarity and attractiveness. | NO<br>No single authority regulating content and therefore, the users have to go through sometimes confusing and illegible content. |
| Cost | **Cheaper**<br>Users pay a monthly fee of CDN $2.8464 [80], which includes a packet transmission charge fee for i-mode service and taxes. *An e-mail of 4KB costs CDN $0.0125.* Also, a content provider's information charge of CDN $2.8464 is charged. Therefore the total is: (2.8464+2.8464) Monthly Fee +(0.0125 ) Data Fee<br>= **$5.7053** | **More Expensive**<br>Users pay a system access fee of CDN $6.73 [77] and emergency service fee of CDN $0.24. *An e-mail of 4KB costs CDN $0.12.* The taxes in Ontario levied are 15%. Therefore, the total is: (6.73+0.24+1.0635(tax)) Monthly Fee +(0.12) Data Fee<br>= **$8.1535** |

**Table G.3 Comparison between content-based and connection-based billing approach.**

Therefore, we can conclude that using i-mode is much cheaper and convenient; thus its popularity. Some phone companies in Canada and the U.S have also started employing this model (charging by volume of data rather than connection time).

# Appendix H

## Practical Examples citing the use of E-payments

In this appendix, we give examples where the use of e-payment mechanisms is better than traditional methods of payments. The e-payments mechanisms referred to have been discussed in previous appendixes B, C, D, E, and F.

**Example case 1: Money needed to be sent to local web programmer.**

Mr. Bob is a local web programmer and he develops a program, which can search for jobs. He advertises his service for $ 10 CDN. All the authorized users will receive an E-mail, which lists all the jobs in demand within the local area. He accepts cash, cheque, money order, and E-mail money transfers. For many people, most convenient mode of payment should be E-mail money transfer. Paying with cash is not feasible for everyone. Payment by cheque has its own cost. Depending on the banks, the minimum processing fee for a cheque typically $1.25. In addition, there are processing time delays for cheques. Canada Post charges $ 3.00 for every money order. Payment by a credit card is also out of question as the user has to first register with credit card providers and also, Bob, has to pay associated transaction fees.

E-mail money transfers charge $1.50 CAD fee. The users can pay up to $1000 CAD at present. The vendor receives payments in less than 24 hrs. The process is secure and reliable. However, the users must first contact the vendor. E-mail money transfer is easy to use. It should be noted that the users would need a bank account before he can start using E-mail money transfer.

**Example case 2: Buy services for a phone.**

The cellular phone companies have come up with many services targeted at cell phone consumers. The services offered at present are ring tones, newscasts, browse internet, and buy products online using mobile phone etc. The charges for services are billed in accordance with the policy of the mobile service providers. As mentioned in the thesis, some charge for the connection time and others for content. For a multitude of services, it is better to charge to the telephone bill rather than paying for each bill individually. With charge to the telephone bill, it

becomes easier to manage accounts. The users has to first register with the mobile phone company for the service.

It is not practical to use credit card to pay for services as mentioned above. As, every merchant will need to registered with the credit card companies. Secondly, service charge incurred would make the use of credit card more expensive. Cash transactions are not convenient. E-mail money transfer levies a transaction fee of $1.50 CAD, still too expensive for the small amount charged. Writing a cheque is not a feasible option as the processing fee of the cheques would be more than the charge for services.

Based on the comparisons as mentioned above, it is our analysis that charge to the phone bill is the best option for the services purchased on the mobile devices.

**Example case 3: Conference registration fees**

A university is organizing a conference requiring registration of participants. The participants have the option of registering by paying by cheque, cash or credit card.

For local participants it may be feasible to pay by cash. However, for out of town participants payment by a cheque or through a credit card will be more convenient. Nevertheless, the cheque may not be convenient for everyone. Also, it takes a long time for the cheque to be mailed and processed. There are risk of cheques being lost during transit.

The users paying through credit card have the benefit of settling the amount at the end of the month or the next billing cycle. Also, the payments are securely conducted using SSL protocol. The participants who pay using the credit card end up paying a small fee. Nevertheless, it offers a reliable and hassle free transaction. In addition, the payment is immediate.

# Bibliography

[1] E.W.Kelly Jr., "The future of electronic money: a regulator's perspective," *IEEE Spectrum, Special issue on Electronic Money,* February 1997, pp.20-22.

[2] Personal information protection and Electronic Documents Act. , "Bill C-6", Clause 7.3, January 1, 2001, http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052bE.html#8, accessed August 2004.

[3] J. Jayavardhane, Overcoming Constraints on Electronic Commerce- Internet Payment Systems," Journal of General Management, Vol. 24 No.2, winter 1998. pg. 19 to pg.35

[4] B. Clifford Neuman and G. Medvinsk, "Requirements for Network payment: The NetCheque Perspective," *IEEE COMPCON'95,* March 1995, pg 32-36.

[5] Federal Reserve Bank of New York. "Fed Point1: How Currency Gets Into Circulation", December 2002, http://www.newyorkfed.org/aboutthefed/fedpoint/fed01.html, accessed Aug-2004.

[6] U.S. Census Bureau, Statistical Abstract, 2003 edition, Section 25, Figure no. 1186 – 1188 http://www.census.gov/prod/2004pubs/03statab/banking.pdf

[7] The Electronic Payment Association, "ACH Network/Rule News", A Billion ACH Payment added in 2002, Orlando, Florida, April 28, 2003.

[8] The Clearing House Inter-Bank Payment System, "Welcome to CHIPS," http://www.chips.org, accessed September 2003.

[9] The Clearing House Inter-Bank Payment System, "Welcome to CHIPS", Annual Stats, Report Date -March 2003, http://www.chips.org/stats.htm, accessed September 2003.

[10] British Broadcasting Company, Inside Out, Credit Card Cloning, July 7, 2003, http://www.bbc.co.uk/insideout/east/series3/credit_card_cloning.shtml, accessed August 2004.

[11] U.S., Public Law, 93-495-October 28, 1974, Article 161, Section e.
http://www.ftc.gov/os/statutes/fcb/fcb.pdf

[12] Machlis S., "IBM hedges its bets on SET," Computerworld. Framingham: Jul 20, 1998. Vol. 32, Issue 29; pg. 4, 1 pgs.

[13] Multos Consortium, Sydney, 2001,
http://www.multos.com/library/pdf/01-08-07%20mcw%20sydney%202001.pdf, accessed August 2004.

[14] K-Y. Lam, S-L. Chung, M. Gu, J-G. Sun, "Security middleware for enhancing interoperability of Public Key Infrastructure," *IEEE Computers and Security,* vol. 22 Issue: 6, September, 2003, pp: 535-546.

[15] J. Iliadis, S. Gritzalis, D. Spinellis, D. Cook, B. Preneel, D. Gritzalis, "Towards a framework for evaluating certificate status information mechanisms," *IEEE Computers Communications,* vol. 26 Issue: 16, October 2003, pp: 1839-1850.

[16] Gutmann, Peter. Encryption and Security Tutorial, University of Auckland, Auckland, New Zealand,http://www.cs.auckland.ac.nz/~pgut001/tutorial/, accessed November 2003.

[17] Rivest R.L, Shamir A, Adleman L.M, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM* (2) 21,*1978*, pp: 120-126.

[18] RSA Laboratories, "RSA Laboratories Frequently Asked Questions About Today's Cryptography," Version 4.1, Section 3.1.1, 2000, RSA Security inc.
http://www.rsasecurity.com/rsalabs/node.asp?id=2152

[19] Massachusetts Institute of Technology, Kerberos
http://web.mit.edu/kerberos/, accessed August 2004.

[20] "On Recent Results for MD2, MD4 and MD5,"RSA Laboratories Bulletin, Number 4-November 12, 1996.
ftp://ftp.rsasecurity.com/pub/pdfs/bulletn4.pdf

[21] Secure Hash Standard, Federal Information Processing Standards Publication 180-2, National Institute of Standards and Technology, August 1, 2002. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

[22] D. Chaum, "Blind Signatures for Untraceable Payments," *Advances in Cryptology Proceedings of Crypto 82*, D. Chaum, R.L. Rivest, & A.T. Sherman (Eds.), Plenum, pp. 199-203.

[23] Johnson, Keith. Office of Patent and Copyright Administration, University of Southern California, Los Angeles, California 90007-4344, U.S.A

[24] Mahony, Peirce,Tewari., Chapter 6, Electronic cash payment systems, Electronic Payment Systems ,Artech House Boston,2001.

[25] Grant N., (2000), "Exploding World of Electronic Checks", Council Presentation, The Electronic Payments Association, http://ecc.nacha.org/resources/resources.htm#CouncilPres accessed July 2004.

[26] NACHA (2002) "NACHA Survey Result on EPS,"
http://ecc.nacha.org/2002_echeck_stats.pdf, accessed June 2004.

[27] Information Networking Institute, "The NetBill Project," Carnegie Mellon Information Networking Institute, 2003, http://www.ini.cmu.edu/NETBILL/, accessed August 2004.

[28] Information Sciences Institute, University of Southern California
http://www.netcheque.org/, accessed August 2004.

[29] CheckFree- The company that powers payment on web, 2003,
http://www.checkfree.com/index.htm, accessed August 2004.

[30] List of e-bills, http://www.checkfree.com/companies.htm, accessed August 2004.

[31] Universal Payment Solutions, 2003
http://www.netchex.com, accessed August 2004.

[32] NetChex Demo, http://www.netchex.com, accessed August 2004.

[33] Universal Payment Solutions, 1999, http://www.universalpaymentsolutions.com, accessed August 2004.

[34] MICR Repository
http://www.asapchecks.com/micr/micr.htm, accessed August 2004.

[35] Dethloff J, (February 1996), "Special Report: Intellectual Property Rights and Smart Card Patents: The Past-The Present-The Future", Smart Card News,
http://www.smartcard.co.uk/resources/articles/prop-rights.html, accessed August 2004.

[36] "Sharp Microelectronics Previews Next Generation Monolithic Smart Card Chip", Press Release, April 22, 2002
http://www.sharpsma.com/sma/pressroom/press.htm?newsid=35, accessed August 2004.

[37] Cagliostro Charles, Smart Card Alliance, 2001, http://www.smartcardalliance.org/industry_info/smart_cards_primer.cfm, accessed August 2004.

[38] Gemplus, 1988, http://www.gemplus.com/, accessed August 2004.

[39] International Organization for Standardization, ISO number 7816, http://www.iso.ch/iso/en/StandardsQueryFormHandler.StandardsQueryFormHandler, accessed August 2004.

[40] MAOSCO Ltd- The Consortium Company, 2002, http://www.multos.com/, accessed August 2004.

[41] MasterCard International, Smart Cards-Mondex, https://hsm2stl101.mastercard.net/public/login/ebusiness/smart_cards/mondex/index.jsp, accessed August 2004.

[42] Visa International, Personal Products, Visa Cash http://international.visa.com/ps/products/vcash/, accessed August 2004.

[43] Danmount http://www.danmoent.dk/pbs/site/pbs_dk/dk/menu_bottom/English?language=en , accessed March 2004.

[44] Common electronic purse specification, 2000, http://www.cepsco.com/, accessed August 2004

[45] The Common electronic purse specifications, Technical Specifications, Version 2.3, March 2001, http://www.epsys.no/ceps/cepstechspecv2.3.pdf, accessed August 2004.

[46] Proton World, 1998, http://www.protonworld.st.com/, accessed on August 2004.

[47] Proton World, http://www.wavxtek.org/Proton.pdf

[48] EMVCo, 1999, http://www.emvco.com/, accessed August 2004.

[49] American Express- Blue, 2004, http://home4.americanexpress.com/blue/blue_homepage_nr.asp?Entry=86, accessed August 2004.

[50] American Express-Private Payments, 2001, http://www.americanexpress.com/privatepayments/, accessed on March 2004.

[51] Gemplus, 1988, Banking Products, Application Cards, http://www.gemplus.com/solutions/banking/download/Multiapplication_Cards.pdf, accessed on August 2004.

[52] Gemplus, 2004, Banking products and Accessories, http://www.gemplus.com/products/banking.html, accessed on August 2004.

[53] CardBase Technologies, News Archive, "CardBase Launches VISA Cash CEPS Compliant product", Cartes 2000, Paris, October 24, 2000, http://www.cardbase.com/news/press_releases/press10.htm, accessed August 2004.

[54] Mahony, Peirce,Tewari. Chapter 4.7, "Secure Electronic Transactions (SET)" Electronic cash payment systems, Electronic Payment Systems, 2'nd Edition, Artech House Boston, 2001.

[55] SET Secure Electronic Transaction Specification, Book 1: Business Description, Version 1.0, May 31, 1997

[56] Loshin, Murphy., Electronic Commerce, "Protocols For the Public Transport of Private Information, Secure Socket Layer", On-line Ordering and Digital Money, 2'nd edition, 1997,

[57] Freier, Karlton, Kocher, Transport Layer Security Working Group, Internet Draft, SSL protocol Version 3.0, November 18, 1996, http://wp.netscape.com/eng/ssl3/draft302.txt, accessed August 2004.

[58] Authorize.Net, 2004, http://www.authorizenet.com/

[59] VeriSign, http://www.verisign.com, accessed August 2004.

[60] VeriSign, Products and Services, Payment Services, Online Payment Processing, Payflow Pro, http://www.signio.com/products/payflow/pro/index.html, accessed August 2004.

[61] Scotia bank, Internet Banking, Online Security http://www.scotiabank.com/cda/content/0,1608,CID418_LIDen,00.html, accessed Aug 2004.

[62] Royal Bank of Canada, RBC and online security, 2001-2004 http://www.rbc.com/security/online.html, accessed Aug 2004

[63] Bank of Montreal, Personal Finances http://www4.bmo.com/personal/0,4344,35649_37015,00.html, accessed Aug 2004

[64] PayPal, 1999-2004, Data Security and Encryption, http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/security-outside, accessed Aug 2004

[65] EyeCash Networks, 2003 http://www.econnectholdings.com/index.html, accessed August 2004

[66] EyeCash Networks, Transaction Flows, 2003 http://www.econnectholdings.com/trans_flow.htm, accessed August 2004

[67] CertaPay, Acxsys Corporation, 2002-2004

http://www.certapay.com/en/, accessed August 2004

[68] eCharge Corporation, eCharge Phone, 1997-2000
http://www.echarge.com/phone/index.html, accessed on August 2004

[69] Open Mobile Alliance (formerly know as wapforum), wireless security, April 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html, accessed August 2004.

[70] Markku-juhani Saarinen, University of Jyvaskyla, Finland,
http://www.jyu.fi/~mjos/wtls.pdf

[71] Entrust Certificate Services, WAP Server Certificates, 2004
http://www.entrust.com/certificate_services/wap_fab.htm

[72] BlackBerry, Security Overview, BlackBerry Security for Wireless Data, 2004
http://www.blackberry.com/products/software/server/exchange/security.shtml, accessed August 2004.

[73] Latest Mobile, GSM, Global, Handset, Base Station and Regional Cellular Statistics, http://www.cellular.co.za/stats/stats-main.htm, accessed August 2004.

[74] Technical_WAP2_0-20020813.zip, WAP-261-WTLS-20010406-a.pdf
http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html, accessed August 2004.

[75] NTT DoCoMo, Press Release Article, March 31, 2004, Tokyo, Japan http://www.nttdocomo.com/presscenter/pressreleases/press/pressrelease.html?param[no]=436, accessed August 2004.

[76] NTT DoCoMo, i-mode global,
http://www.nttdocomo.com/corebiz/imode/global/index.html, accessed August 2004.

[77] Fido Home, Packages and Services, Data services and Internet access http://www.fido.ca/portal/en/packages/datapackages.shtml, accessed August 2004.

[78] Open Mobile Alliance, Technical Section, Software Platform Components http://www.openmobilealliance.org/tech/profiles/ccppschema-20030226.html, accessed August 2004.

[79] NTT DoCoMo, i-mode, http://www.nttdocomo.co.jp/english/p_s/i/index.html, accessed August 2004.

[80] NTT DoCoMo, Business Strategy, Simple, and Affordable Pricing System, http://www.nttdocomo.com/corebiz/imode/why/strategy.html, accessed August 2004.