1997

# The development and use of the Secure Electronic Transaction (SET) protocol on the internet

Damon James Whyte
*Edith Cowan University*

# Edith Cowan University

# Copyright Warning

# The Development and Use of the Secure Electronic Transaction (SET) Protocol on the Internet.

By

**Damon James Whyte**

**Supervisor: Dr Timo Vuori**

**An Honours Thesis Submitted to the**
**Faculty of Science, Technology and Engineering**
**Edith Cowan University**
**Perth, Western Australia**

**Submission Date: 5 December, 1997**

**In fulfillment of the requirements for the degree**
**of**
**Bachelor of Science (Computer Science) Honours**

# USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

# Abstract

While still in its infancy, Electronic Commerce is growing at an exponential rate each year (Watson, 1997, p.53). Although few doubt that such growth will only continue in years to come, many people still have serious reservations about the levels of security offered by currently available applications for conducting such trade. This thesis identifies some of the key areas of concern regarding Electronic Commerce on the Internet, and looks at the ways in which the Secure Electronic Transaction (SET) model, proposed by MasterCard and Visa, succeeds or fails in addressing these concerns. It identifies and describes the key elements and primary functions of the SET protocols in a manner that will enable students and other interested parties to understand these protocols quickly and easily.

# Declaration

I certify that this document does not incorporate, without acknowledgement, any material previously submitted for a degree or diploma in any institution of higher education and that, to the best of my knowledge and belief, it does not contain any material previously published or written by another person except where due reference is made in the text.

Signature

Date : 5/12/97

# Acknowledgements

First and foremost, I wish to thank Vicki, my beloved wife-to-be, for her continuous love and support from afar throughout a very trying year. Likewise, I wish to thank my family, particularly my mother Lydia, for always supporting me in whatever I choose to do, regardless of the consequences. Finally, I wish to thank my supervisor, Dr Timo Vuori, for his help and patience, and for teaching me that structure does not "just happen".

# Table of Contents

# Table of Figures

# 1. Introduction

Many of the major transitional periods in history have been influenced by the development of new or improved avenues of communication, trade and production. Today we live in a highly consumer oriented world, in which trade directly influences not only our individual lifestyles, but the stability and affluence of our economic and political systems as a whole.

## 1.1. Background of Thesis

In recent years the constant increase in the availability of cost-effective technology has lead to whole new vistas of potential consumerism and communication. We are rapidly approaching a time where even the smallest of merchants will be able to market their goods or services to individuals all over the world, and where producers and wholesalers may suddenly find it cost-effective to bypass retailers all together and market themselves directly to the public. All of this is primarily the result of the global communications network now known as the Internet. The Internet is allowing businesses of all descriptions to communicate with a broader range of consumers, using the power of computer-based multimedia.

The capacity for businesses to instantaneously communicate data and information with other offices, businesses and consumers, across vast distances is revolutionising established working practices. By using the computerised communications network that now spans the globe, information can be shared across corporate, geographic and political boundaries with the greatest of ease. Virtual organisations (as described in Section 2.3.1.) are now becoming a reality.

This capacity to do business electronically, known as Electronic Commerce, is changing the face of business, providing enormous opportunities for those who take advantage of it. There is little doubt that many new fortunes will be made, and many others will change hands as the race for mastery of the global economic community is run. Projections for the growth of Electronic Commerce indicate that by the year 2000 such transactions could reach up to US$30 billion per annum (Somlyody, 1996, [on-line]).

## 1.2. Significance of Thesis

With any new form of communication there are always problems that need to be addressed through the development of appropriate procedures, protocols and standards. The rapid development of the Internet, and its phenomenal popularity and use, has created an environment filled with both paranoia and legitimate concerns as to the security and privacy offered to users. The Internet is an open system, with a dynamic number of users, no universal regulation, and a seeming lawlessness that rivals the Wild West of old. It is natural enough then that one of the major issues that commercial users of the Internet are concerned about is security (Ford & Baum, 1997, p. 2). It is predominantly this issue and some of the possible solutions thereof, with which this thesis will deal.

The Secure Electronic Transaction (SET) specification defines new protocols that could potentially address this issue. SET is a specification for an application-level protocol that appears to provide a secure methodology for payment card transactions over the Internet. "Payment cards" include credit cards, debit cards, and all forms of proprietary payment cards offered by private companies and organisations. Masterminded by Visa and MasterCard, version 1.0 of the SET specifications was released on May 31st, 1997.

If successful, SET will probably be adopted by most, if not all, of the major payment card brands as the industry standard for secure payment card transactions over the Internet. Indeed, apart from MasterCard and Visa, several other significant payment card brands have already declared their support, including American Express, the third largest in the world ("Visa and MasterCard welcome American Express", 1996, [on-line]).

Payment cards are one of the very few non Internet-specific forms of payment available for electronic transactions on the Internet (see Appendix A for alternate Internet payment methods). As many people already have payment cards, and many merchants already accept them, it would seem logical that consumers are unlikely to be desirous of having to learn how to use new and unorthodox forms of payment. Because of this, a standard that provides for secure payment card transactions across the Internet is obviously highly desirable for both consumers and merchants alike.

By providing an objective overview of the primary security concerns related to Electronic Commerce, and reviewing the effectiveness of the SET protocols, both on its own merits and compared to the existing defacto standard, this thesis will clarify the progress being made in this area, and the current directions of the industry.

## 1.3. Purpose of Thesis

This thesis gives a brief overview of the factors that have lead Electronic Commerce to develop to its current state. The significant security issues are identified, and how they are addressed by both the current standard protocol (Secure Sockets Layer) and the SET protocols will be discussed. However, the main aim of the thesis is a review of the key

elements and functions of the SET protocols, and their effectiveness in addressing some of the primary areas of concern relating to secure Electronic Commerce on the Internet.

## 1.4. Research Questions

In order to appreciate the scope and consequent difficulties involved in doing definitive work in the area of Electronic Commerce, it is necessary to appreciate the number of different fields that impinge upon it. At the highest level of abstraction, technical requirements, political and legal boundaries, economic constraints, and moral and ethical values and systems influence the issues involved.

The focus of the research in this thesis is the effectiveness of the SET protocols in addressing the security of payment card transactions on the Internet. Consequently, the primary questions to be addressed in the thesis are:

- What are the commonly accepted concerns regarding the security of consumer-based Electronic Commerce on the Internet?
- What are the key elements and functions of the SET model?
- Do the SET protocols adequately address the security concerns identified, either partially or in full?
- How does the security offered by SET compare to that of the current defacto standard (SSL).

## 1.5. Scope of Thesis

Concerns regarding the security of Electronic Commerce are many and varied, ranging from purely technical aspects of implementation through to the sociological impact that Electronic Commerce is going to have on the global community. This thesis focuses on

security concerns that can be addressed through the adoption of suitable technical standards. In some cases this includes non-technical issues, although such issues are in the minority of those addressed.

The thesis describes the effectiveness of the SET protocols in addressing the primary areas of concern related to secure Electronic Commerce, as are generally accepted by the majority of the associated contemporary literature. Unfortunately, the relatively short amount of time available for the preparation of an Honours thesis has precluded the in-depth study of a number of related areas.

The implementation specifics of the SET protocols have not been discussed, which has lead to the omission of in-depth discussion on a number of issues. These include associated problem areas that are currently outside the scope of the specifications, such as "Denial of Service" attacks, and the possible integration of SET into other developing technologies such as smart cards.

The entire Electronic Commerce revolution, and all the associated areas such as networking technologies, communication protocols, authentication systems and technologies, law, ethics and privacy policies, payment methods and infrastructures, and many others, are all progressing at an ever increasing rate of development. It would be impossible to provide sufficient discussion on all these topics without many years of involved research. Consequently, this thesis has been constrained to providing the reader with a comprehensive understanding of the issues that much of the work in these areas is trying to address, and the efficacy of the SET protocols in doing so.

## 1.6. Structure of Thesis

Chapter 2 gives a brief overview of the current state of Electronic Commerce. It looks briefly at the Internet, and at Electronic Data Interchange, the principal forerunner to the broader form of Electronic Commerce that we know today. However, the primary focus is on secure retail electronic transactions, which is the area that the SET protocols are primarily concerned with. The discussion is extended to cover some of the more atypical payment methods proposed or currently available on the Internet, some of the problems perceived with the current systems, and the nature of a typical transaction.

Chapter 3 discusses encryption, one of the more powerful tools for protecting data on the Internet. Encryption is certainly nothing new to many people, but modern cryptographic techniques, utilising the processing power of computers, are proving to be the cornerstone on which most "secure" software is built. This chapter looks at *secret key* and *public key* methods, two significant forms of encryption currently in use. Additionally, it describes some of the more useful techniques that are utilised in combination with encryption, like *digital signatures* and *message digests*, which are significant elements in security protocols such as SET and the Secure Sockets Layer (SSL).

The basic functionality of the SSL is discussed in Chapter 4. SSL is widely accepted as the current defacto security protocol for the Internet. Despite this, SSL was not designed with Electronic Commerce specifically in mind, and consequently has a number of limitations when used for this kind of transaction.

Chapter 5 looks at the specifics of the SET protocols. It outlines the objectives and scope of SET, and identifies the key participants, elements and processes involved in a SET transaction. The cryptographic techniques employed by SET are described, including the introduction of dual signatures, a new technique introduced for the first time in the SET specifications ("Secure Electronic Transaction (SET) Specification Book 1: Business Description", 1997, [on-line]), hereafter known as the SET Business Description (1997). The use of digital certificates in SET is discussed, as is the "hierarchy of trust" required for SET compliant certificate authorities.

Chapter 6 then looks at the overall effectiveness of SET, and compares its efficacy with that of SSL as a security protocol for Electronic Commerce transactions. The comparative criteria are based on the key requirements of electronic payment systems (see Chapter 2), and include authentication, compatibility, payment security, information integrity and non-repudiation.

A summary of the significant conclusions that can be drawn from the thesis is contained in Chapter 7. The key issues that have been identified within the thesis are recapped in a manner that clearly identifies the relative strengths and weaknesses of payment cards in general, as well as outlining the broader issues that require further research.

# 2. Contemporary Electronic Commerce

Electronic Commerce as we know it today is probably better known for its problems than its benefits. The public is being bombarded with horror stories that focus on either the dangers of elusive computer criminals (Ford & Baum, 1997, p. 3), or on the supposed totalitarian state that Big Brother is surreptitiously ushering in behind the scenes (Bacard, n.d., [on-line]). Consequently, despite the general apathy that pervades our society, people aren't quite ready to sit back and put their own finances on the line until they're sure it's safe to do so ("Electronic Commerce", 1997, [on-line]).

Many potential participants in Electronic Commerce on the Internet currently feel that they have something to worry about (Driscoll, Jain, Lyons, Nuckols & Roberts, 1997, [on-line]). The public want personal privacy, the merchants want to be protected against fraud, and everyone with a direct connection to the Internet wants to be sure that their system is safe against unauthorised entry (Scollay, 1997, [on-line]). This chapter briefly outlines the development of the Internet and Electronic Commerce, and discusses a few of the more significant topics and issues related to these areas.

## 2.1. Electronic Data Interchange (EDI)

In order for the international business community to take advantage of electronic communication, it first needed to develop a standardised data format. This would enable various computers in different geographical locations, and possibly running completely different operating systems and/or applications, to exchange data and seamlessly integrate it into their own systems.

Forward thinking companies who pioneered various techniques for transferring data in formats that could be processed on receipt had no guarantees that the idea would be embraced by other businesses. Their efforts have been described as an "act of blind faith" ("A Brief History of Electronic Commerce", 1996, [on-line]). This was prior to anyone using the terms Electronic Commerce or Electronic Data Interchange (EDI). The understanding that such common formats were necessary lead to the inception of associated standards bodies in Europe and the USA.

EDI can be summed up as the exchange of standards-based, structured data between computer applications. The obvious advantage of this is that the exchanged data can be moved between systems without the need for rekeying. "Because it can speed the flow of information and pass data automatically to other automated applications, EDI is a powerful tool for improving business processes." (Morell, Neal & Fries, 1995, [on-line]).

A number of Value Added Networks (VAN) were created in the eighties, targeting major industry groups, in an attempt to generate significant industry interest in EDI, which was claimed to reduce traditional business processing costs by around 66%. However, it was only with the advent of the Internet as a commercial network that widespread interest in EDI was observed. The primary reason for this was the estimation that Internet based EDI would decrease the cost of conventional business procedures by a further 66% on standard EDI savings (Watson, 1997, p. 55).

## 2.2. The Internet

The first real step towards the Internet as we know it today was in 1969, when the US Defense Advanced Research Projects Agency (DARPA) was commissioned to research network protocols. As a result of their work, in 1973 the Transmission Control Protocol/Internet Protocol (TCP/IP) was recommended as a standard networking protocol for computer network communication. According to Bruce & Dempsey (1997), the popularity of TCP/IP rose sharply in 1983 when the version of UNIX released by the University of California at Berkley included this network protocol. This lead to TCP/IP becoming the defacto standard.

In 1986, the National Science Foundation (NSF) decided to network their nationwide supercomputer sites in order to improve efficiency. The high-speed network used to connect the NSF supercomputers formed the backbone of the Internet, although the term *backbone* is often used in a more general manner to include high-capacity telephone links, microwaves, lasers, fibre optics, and satellites, connecting networks, computer sites, and people (Eddings, 1994, p. 9). Today the Internet has evolved into a shared network, connecting businesses, universities and private homes all over the world.

The term Internet is used to describe the common network communications, and is actually made up of various services that use the TCP/IP protocols (Bruce & Dempsey, 1997, p. 220). TCP/IP is actually a number of different protocols, with different functions, bundled together. At the center of this web of protocols is the Internet Protocol (IP), which is a packet multiplexer. "Messages from higher level protocols

have an *IP Header* prepended to them. They are then sent to the appropriate *device driver* for transmission." (Cheswick & Bellovin, 1994, p. 19).

One of the key benefits derived from the nature of TCP/IP is its robustness. The web-like nature of the Internet means that TCP/IP can channel data through a wide range of alternate nodes when transmitting from point A to point B. There are many different paths through which the data can flow, consequently, the network as a whole can suffer massive degradation and still keep functioning. Obviously, this was a highly desirable attribute where the Department of Defense was concerned. However, this very attribute is also one of the main security weaknesses of the Internet (Pfleeger, 1997, p. 390).

One of the more recently developed Internet services, and certainly the best known, is the World Wide Web (WWW), a simple, browser based graphical user interface providing point-and-click navigation of the entire Internet. With improvements in browser technology, the WWW is providing a simple, yet effective, multimedia platform from which anyone can participate on the Internet.

According to Tom Miller (1997) of the Emerging Technologies Research Group, the number of adult users of the Internet in the USA alone exceeds 40 million, with over 30 million of those using the WWW. The USA is estimated to contain the majority of Internet connected households, with approximately 66% of the worldwide total. The remainder is fairly evenly split between Europe and the Australasian/Pacific region ("Geographics", 1997, [on-line]). According to this particular survey, current predictions are for the total number of Internet users to triple by the year 2000.

Of course it must be noted that it is notoriously difficult to get consistent statistics regarding Internet user demographics, as each different survey uses its own criteria. Factors that can vary include; whether a person actually uses the Internet, or merely has access, the timeframe within which the user must have logged on last, and whether the access is from home, work, or both. Nevertheless, the one inescapable fact is that the Internet, and in particular the WWW, is changing the way in which a growing number of people communicate and otherwise interact with the global community as a whole. Time and geographical location are no longer significant barriers to like-minded individuals of all persuasions sharing thoughts and ideas, or conducting business.

## 2.3. Electronic Commerce

The term Electronic Commerce is a relatively new one, and can be considered to stem from a broadening of EDI. It evolved from the realisation that if a wider variety of messaging solutions were available, then far more could be gained from network communications than simply the exchange of raw data ("Some definitions of Electronic Commerce", 1996, [on-line]).

In broad terms Electronic Commerce is the conduct of business using a combination of structured and unstructured message exchange (EDI and e-mail), as well as binary data exchange, shared data, databases and database access, across the entire range of networking technologies, and across both public and private sectors ("ECA - Aims and Objectives", n.d., [on-line]). "As the Internet has proved, we now live in a global community.... We can do business with anyone, anywhere in the world, at any time." ("Changing the Way you do Business", 1996, [on-line]).

Essentially there are two distinct areas within Electronic Commerce. The first is the capacity for businesses to communicate information between their offices, suppliers and business partners. This type of inter-business Electronic Commerce is embodied by standards such as EDI, which is a subset of Electronic Commerce describing purely inter-process (computer to computer) communication (Houser, 1995, [on-line]).

The second type of Electronic Commerce is the ability for businesses to directly market their goods or services to a wider range of consumers. Essentially, wholesale and retail sales.

Electronic Commerce as a whole recognises the additional need for inter-personal (human to human) communication, funds transfers, and file sharing (Houser, 1995, [on-line]). In either case, according to Watson (1997), it is not a matter whether businesses should be on the Internet or not, but rather a matter of how and when.

### 2.3.1. Inter-business Electronic Commerce

Business is largely about the right people having the right information at the right time. This often means simply staying in communication with geographically separate components of the business ("Changing the Way you do Business", 1996, [on-line]). The functions such inter-business communication is currently used for include; the updating of stock, orders and financial data, compilation and exchange of statistical information, exchange of graphics, voice and video data, and the facility to work on designs or common documents ("Some Definitions of Electronic Commerce", 1996, [on-line]).

Indeed, the constant improvement of the global telecommunications networks, enabling virtually instantaneous data exchange, have lead the business community to completely re-evaluate traditional strategies and philosophies. It is not enough for businesses simply to "upgrade" their technology to utilise Electronic Commerce; they must be willing to embrace new work practices if they wish to do more than merely streamline what already exists ("The Future", 1996, [on-line]). If businesses try to take shortcuts in introducing the concept of Electronic Commerce to their existing structure, that is to say that they fail to adopt appropriate work practices that capitalise on it, they run the risk of spending money for little or no gain ("Business Process Redesign", 1996, [on-line]).

In the document "Changing the Way you do Business" (1996) the author(s) identify three key steps commonly implemented in order to successfully expand an existing business into the world of Electronic Commerce.

1. Introduce electronic alternatives to existing manual and paper-based operations.
2. Consider, adapt and simplify the information flows.
3. Use the improved information flows in new and dynamic ways.

It should be noted that "information flows" does not simply refer to computer-to-computer communication. Predominantly it refers to the way information is used and distributed in combination with the adoption of Flexible Working practices. Such practices can include; telecommuting, distributed offices, mobile workers, virtual teams, desk sharing, job sharing, flexible or part time working hours, carer breaks, or even complete relocation of business ("Flexible Working", 1996, [on-line]).

Electronic Commerce is about consumers, businesses and business partners being able to share information electronically, thereby improving the efficiency, economy and competitiveness of business practices.

### 2.3.2. Consumer-based Electronic Commerce

The relatively recent advent of the WWW platform has brought a sizeable portion of the world population "online" virtually overnight. Suddenly any business with a few spare dollars can market themselves, potentially, to upwards of 45 million people all over the world, 24 hours a day, 365 days a year. In addition to the number of potential consumers, there is also the fact that a large number of Internet users have particularly attractive demographics from the perspective of merchants, i.e. age, income, education, etc. ("CommerceNet / Nielsen Internet Demographics Survey", 1997, [on-line]).

It would seem reasonable that as more people gain access to this developing marketplace, and as stable and secure financial services are developed to service it, the WWW will become increasingly consumer-driven. It is estimated that 21% of the current users of the WWW already have and continue to purchase goods electronically (Miller, 1997, [on-line]).

New "electronic shopfronts" are springing up daily, marketing a wide range of goods and services to the world. The WWW now provides a rich multimedia environment, enabling marketers to realise the full possible impact of the advertising dollars they spend. The services that can be provided online can include functions like; consumers choosing from the goods or services offered, order and delivery details, after sales service facilities, and payment procedures. One of the key advantages of the Internet as

a forum for Electronic Commerce is that when a merchant updates information such as stock, prices, special offers, or any other information for customers, such changes are usually immediately available to consumers ("The Possibilities with Electronic Commerce", n.d., [on-line]).

From the consumer's point of view, Electronic Commerce has many potential advantages to offer over more traditional methods of buying. Apart from a potentially enormous marketplace, increased physical safety (Watson, 1997, p. 52), and the obvious multifarious benefits in terms of time, effort and improved service (Ford & Baum, 1997, p. 2), Electronic Commerce can also be used to "personalise" shopping. Data about an individual's visit to a site can be stored for use against future visits. For example, if you bought a Computer Science textbook from a WWW bookshop, the next time you visited that site the web server might choose to show you any specials on Computer Science texts when you arrive. Likewise, frequent customers might be given discounts or other special offers automatically.

Nevertheless, despite all the promise that this type of commerce holds, many people still have serious reservations about the ease and safety of using it (Hoffman, Novak & Chatterjee, 1995, [on-line]). The bottom line still remains the same; if Electronic Commerce is to fulfil its potential, methods for conducting electronic payments must be universal, automated, convenient and, of course, secure.

### 2.3.3. Payment Alternatives

With the ever-increasing popularity of the Internet, the viability of this new medium as a potential tool for commerce is becoming almost impossible to ignore. As a

consequence, many innovative merchants and banks are starting to move quickly to establish themselves as pioneers in the marketplace, and so gain an advantage over their competitors ("SET Business Description", 1997, p. 1).

Although the exact nature of commerce on the Internet is yet to be clearly defined, what is clear is that "wherever there are electronic [monetary] transactions, financial institutions have a major stake - particularly in the face of non-traditional competition." ("Acquiring Internet Transactions", n.d., [on-line]). In the SET Business Description (1997), MasterCard and Visa allude to the fact that financial institutions have a vested interest in the rapid growth of Electronic Commerce. This is because a much higher percentage of the associated transactions will use payment card products than cheques or cash.

Thus far there have been a number of payment schemes implemented for transactions across the Internet. "The first payments for services on the Internet were conventional ones. Subscribers transferred monthly fees for a service from their bank-account into the accounts of the selling party." ("Money on the Internet", n.d., [on-line]). This method of payment was slow, expensive and relatively inefficient, especially when dealing with merchants in other countries.

Next came payment card transactions, complete with all the associated security issues. An early attempt to resolve some of these issues saw the introduction of third party companies ("Money on the Internet", n.d., [on-line]). These companies collect and approve payments between clients, and then bill the clients for their total accumulated

expenditure on a periodic basis, removing the necessity of making multiple payment card payments for possibly insignificant amounts.

The use of third party companies, or even simply the use of payment cards themselves, can lead to potential violations of privacy. If details of individual payment card transactions are gathered in one centralised system, including where, when and what is purchased, this data can be used to tell much about the person involved, and can conflict with the individual's right to privacy ("Money on the Internet", n.d., [on-line]).

According to Neuman & Medvinsky (1995), the important characteristics that an Internet payment infrastructure must provide include security, reliability, scalability, anonymity, acceptability, customer base, flexibility, convertibility, efficiency, and ease of use. These can be described as follows:

**Security** – Information is power in many cases, and often financial information most of all. Because of the sensitive nature of much of the information contained in financial Internet transactions, they are likely targets for computer criminals. Due to the open nature (accessibility) of the Internet, a high degree of security is required for such transactions.

**Reliability** – If we continue to see the exponential growth of Electronic Commerce that we have witnessed thus far, the reliability of payment systems will become increasingly critical to the functionality of not only individual businesses, but also, potentially, whole economies. The more critical this payment infrastructure becomes, the more likely a target it also becomes for vandals and subversives. These systems will need to be

robust, with substantial redundancy built into them. Thankfully, by its very nature the Internet does much to support this exact requirement (see Section 2.2).

**Scalability** – Obviously, any payment system implemented on the Internet must support the potential for substantial growth. Any system that depends on central payment servers is probably going to have limited growth potential, and will likely suffer degradation of performance as the number of users and merchants grows.

**Anonymity** – The privacy of individual spending patterns needs to be protected from sources outside the financial institutions involved in a given transaction. Under some payment schemes it is impossible for consumers not to identify themselves to acquiring financial institutions when purchasing goods or services. However, it may occasionally be desirable for a consumer to maintain their anonymity to any other parties. Any successful payment schemes are likely to be able to provide this anonymity when required.

**Acceptability** and **Customer base** -- The more widely accepted a method of payment is, the more useful it is to those who have it. If a payment system is widely held by consumers, but only accepted by relatively few merchants, then it is probably doomed to be superceded by a more widely accepted method of payment. The same is conversely true of merchants. If a payment system is widely accepted by merchants, but is used by few consumers, then the same result is likely. Likewise, if a payment system is accepted by a variety of separate payment servers, these servers must be able transact payments with each other, otherwise the usefulness of the payment system is restricted.

**Flexibility** – A comprehensive payment infrastructure for the Internet would probably need to support a variety of transaction types, analogous to more traditional payment options such as cash, cheques and payment cards. These will be necessary to support the differing requirements of each transaction, i.e. anonymity, speed, size of transaction, auditability, and so on.

**Convertibility** – Because each individual consumer will require some or all of the above different transaction types, it follows that there will certainly be a requirement that one form of funds within the overall payment infrastructure be convertible to any other form with minimal effort.

**Efficiency** and **Ease of use** – Because some payments on the Internet are bound to be very small, possibly in the order of a few cents, a method of payment is required that has transaction costs economic enough to meet such payments without being noticed. Additionally, payments of this magnitude should be able to be made automatically and without loss of performance, although the user should be able to monitor his/her spending at all times, and should have to manually authorise payments exceeding a set amount.

**Ease of implementation** – Ideally, an application level protocol should be developed to allow not only payment services of the same type to interact, but payment services of all types. This would enable developers to only have to worry about meeting one set of communication protocol requirements, with a standard level of service available to higher level applications.

There are presently a substantial number of existing or proposed electronic payment schemes and products available, with more appearing on a regular basis. A table containing references to information on many of these schemes and/or research lists is given in Appendix A.

Obviously, it is not practical to outline all of these methods herein. Instead, the following sub-sections outline a few of the better known and more generic payment systems that currently exist on the Internet. These systems typify the concepts embodied by many other similar payment schemes, and can be classified into three general categories:

1. Electronic currency systems (ecash)
2. Credit-debit systems (NetCheque)
3. Secure payment card systems (CyberCash).

### 2.3.4. ecash

DigiCash's *ecash* is purported to be the digital equivalent of cash, and is a good example of electronic currency. Users can withdraw "digital coins" from their Internet bank account and store them on their hard disk. According to DigiCash ("An Introduction to ecash", 1997, [on-line]), ecash offers payment that is fast, anonymous, and traceable.

According to Neuman and Medvinsky (1995), users of electronic currency have to first establish an account with a currency server on the Internet. They can then purchase currency certificates through this account, or by using credit cards, electronic cheques,

or paper money through reverse teller machines. Once issued, the currency certificates represent a set value, which can be spent with merchants who accept them, or deposited into other accounts on similar currency servers.

Perhaps the most attractive aspect of the ecash concept is the anonymity that it offers. Unlike other methods of payment, there is no requirement for a purchaser to divulge any more information about their identity than they wish ("The Ease of Using ecash", 1997, [on-line]). Like hard currency, ecash has its own intrinsic value.

Anonymity comes from the fact that it is extremely difficult to determine to whom a currency certificate was issued, and under some models it is virtually impossible to do so. However, because DigiCash keeps a database of spent certificates, if a user attempts to spend the same certificate twice, they will surrender enough information to be identified (Neuman & Medvinsky, (1995), [on-line]). This same database provides the information that can be used as proof of payment should disputes arise between payer and payee.

The idea behind ecash is to provide people with a form of electronic currency that they can use as they would normal hard currency. Withdrawals from ecash accounts are password protected, and public key encryption (see Chapter 3) is used whenever ecash is transferred across the Internet. In addition, ecash can be stored on Smart cards, allowing you to carry your electronic currency with you ("Money on the Internet", n.d., [on-line]).

The ecash "Cyberbucks" trial was initiated in October 1994, and included over 100 merchants and 25,000 users. A number of ecash licenses have been sold to banks. Such licenses are non-exclusive, consequently allowing banks to determine their own competitive pricing structure when issuing ecash. There are six banks that presently issue ecash, including Australia's own Challenge Bank ("Current ecash Issuers and Other Licensees", 1997, [on-line]).

The techniques used to keep track of certificates in order to stop double spending vary between different electronic currency implementations. Some track currency certificates that have been spent, while others track certificates which have been issued but not yet spent. In either case, this massive overhead in terms of maintaining large databases is one key disadvantage of electronic currency. Another is that users are forced to acquire and maintain Internet bank accounts with currency servers (Neuman & Medvinsky, (1995), [on-line]).

### 2.3.5. NetCheque

NetCheque is a credit-debit system designed primarily by Clifford Neuman of the Information Sciences Institute at the University of Southern California. NetCheque certificates (cheques) contain similar information to paper cheques, and are designed to work in a similar fashion. According to Mankin (1994), each cheque contains the name of the payer, the name of the financial institution, the payer's account number, the name of the payee and the amount of the check.

The cheques are signed by the payer using a digital signature, and must also be signed by the payee before they can be cleared. This provides a means for the auditing of

payments. Users of this system are required to establish "cheque accounts" on accounting servers (Neuman & Medvinsky, (1995), [on-line]). Once a cheque is presented for payment, the payee's accounting server attaches its own endorsement certificate and passes the cheque on to the issuing server. If this server is not registered as a trusted server, the cheque is passed to an intermediate trusted server, which then attaches its own endorsement, and so on. Once the cheque reaches the issuing server the endorsements are used to channel the funds back to the payee's account.

According to Neuman & Medvinsky (1995), this clearing between servers allows organisations to set up accounts in their own in-house accounting servers, with accounts corresponding to budget lines. Authorised signers write cheques against these accounts, while the organisation maintains a single account with an outside bank.

The NetCheque system is based on Kerberos (Neuman & Medvinsky, (1995), [on-line]), a Data Encryption Standard (DES) based Authentication System. While Kerberos itself is fairly widely used, it does have some limitations that make it unsuitable as a sole basis for secure Electronic Commerce on the Internet (Neuman & Ts'o, 1996, [on-line]).

### 2.3.6. CyberCash

According to CyberCash, Inc. ("CyberCash Overview", 1997, [on-line]), *CyberCash* system cardholders are issued with an electronic wallet in which they can store payment card information. When the cardholder wishes to make a purchase, they click on the card they want to use, and the details are transmitted accordingly. The wallet is password protected, and all details transmitted across the Internet are strongly encrypted using a combination secret key and public key encryption, as described in Chapter 3.

All merchants who wish to accept CyberCash are screened for authenticity and reliability before being allowed to do so, offering consumers some protection against merchant fraud ("Acquiring Internet Transactions", n.d., [on-line]).

In general terms, one of the advantages that payment cards offer over alternate payment methods is that there is no requirement for users to establish new financial accounts online (Neuman & Medvinsky, 1995, [on-line]).

### 2.3.7. Areas of Concern

The barriers to the widespread acceptance of Electronic Commerce are many and varied. Certainly one of the main areas of concern with the Internet as a whole is that of security. Until fairly recently there were few real safeguards to ensure that messages sent across the Internet had not been intercepted, read, or altered whilst in transit. ("Why Do We Need Security in Cyberspace?", n.d., [on-line]).

The potential for fraud and deception on the Internet is fearsome. The Internet's massive connectivity and availability, combined with inexperienced or just lazy system administration on many hosts, allows criminals to find and exploit weaknesses. When information is sent over the Internet, there is usually no way for a user to know in advance how many or which other systems this information might pass through on the way. If even one of these systems is compromised, then the information may be at risk. If a consumer's personal financial information were to fall into the hands of a criminal, there would be little to stop that criminal from posing as the individual and using the information to make purchases through mail order, telephone order or any other non-

authenticated "face-to-face" ordering systems (Hoffman, Novak & Peralta, 1997, [on-line]).

Although many variations exist, a typical retail electronic transaction could be described as having the following steps (Computer Technology Research Corp., 1996, p. 137):

1. A consumer finds a merchant's site that contains goods of interest, and then either browses the merchandise on display, or possibly downloads a catalogue for viewing off-line. It should be mentioned that some merchants have begun the practice of producing off-line catalogues that can be distributed to their customers through standard channels, such as the postal system, which can then be used to create order forms that are sent to their electronic shop. This is in order to reduce bandwidth usage of their site, consequently reducing both the load on their server, providing faster service, and reducing their own costs.

2. When the consumer finds goods or services they wish to purchase, they download an order form, if they haven't already obtained one by other means such as a catalogue. Once this form has been completed, including payment and delivery details, it is then forwarded to the merchant for processing.

3. Once the merchant has ascertained that he/she can fill the order, they would usually send a confirmation note back to the customer, and process the payment information as per a standard Mail Order/Telephone Order (MOTO) transaction. The exact point at which the goods are dispatched varies with the merchant, but for payment card transactions it would usually be immediately.

The security concerns that are notable in the process described above can be summarised as follows:

1. How does a consumer know that the supposed merchant is indeed a legitimate vendor who:
    - In reality, is who they say they are.
    - Owns the goods for sale, and is authorised to sell them.
    - Can accept the payment method they wish to use, and will not use it for fraudulent purposes at a later date.

2. How does a merchant know that the consumer is:
    - Who they say they are.
    - The legitimate holder/owner of the payment method used.

3. How does either party know that the messages sent and received have not been:
    - Intercepted and read by a third party.
    - Altered in transit.

4. Additional problems include:
    - Verification of the exchange.

As can be observed, striking a balance between allowing privacy of information, and anonymity where required, while at the same time providing enough information to authenticate the identities and authority of the parties involved, and to provide verification of the transaction, is a significant problem.

From the perspective of Internet businesses, one major concern is ease of use. No matter what security techniques and payment meth ds are offered to assuage consumer concerns regarding lack of security, they must be easy to use or they are unlikely to gain widespread acceptance. The conflict between message security, authentication, privacy and ease of use is probably the pivotal issue facing the world of Electronic Commerce.

There are many other technical issues relating to Electronic Commerce, which are of concern to anyone who has a system connected to the Internet. These concerns focus primarily on restricting who and what has access to an organisations primary host, that is, the server that acts as the connection between internal networks and the Internet (Sheldon, 1997, p. 434).

Although secure payment gateways (intermediate financial servers) are an assumption in most electronic payment schemes, the associated issues and implementation of such servers are beyond the scope of this thesis. For more information on this topic Bruce & Dempsey (1997), Cheswick & Bellovin (1994), Pfleeger (1997), Stallings (1995), and White, Fisch & Pooch (1996) are recommend by the author as good background sources.

# 3. Cryptography

The most practical way to protect information being sent over an open network like the Internet is to use cryptographic techniques to encrypt messages. These techniques render the information contained therein unusable to anyone except the intended recipient, or possibly an extremely sophisticated adversary.

Cryptography is the science of sending messages in a coded format. The word itself stems from the Latin *kryptos*, meaning "hidden", and *graphos*, meaning "writing". When we take an ordinary message, usually called *plaintext* or *cleartext*, and *encrypt* it, we convert it into what appears to be gibberish to the untrained eye. This encrypted version of the original message is usually called *ciphertext* or a *cryptogram*. The mathematical formula or rules that allow a person to switch back and forth from cleartext to ciphertext and vice versa are called a *cipher* or an *algorithm* (Bacard, 1995, p. 70).

The objective of cryptography is to enable two people to communicate over a potentially insecure channel in such a way that an opponent who intercepts the message cannot understand what is being said (Stinson, 1995, p. 1). According to Bacard (1995), strictly speaking, any form of communication that is not commonly used or understood can be considered a form of cryptography. He points out that historically the use of alternate forms of language is a good example of this. Ancient Egypt had two distinct and well-defined languages, the hieratic, known only to the priesthood, and the demotic, used by everyone else. Similarly, there are records of the ancient Greeks developing forms of shorthand. Indeed, for nearly a thousand years after the life of Christ, the

ruling elite of Europe communicated in Latin, a purely scholarly language at the time. Modern cryptographics can be viewed as a language composed of mathematical formulas of such complexity that only the highly skilled, aided by modern technology, have any reasonable chance of interpreting.

Modern encryption techniques ensure greater security through the use of a unique *key* (Schneier, 1994, p. 130). A key can be any value that can be represented in the key length used, i.e. the number of bits used to represent the key. The key is used in combination with the encryption algorithm to encrypt plaintext messages. Fundamentally, the longer the key is, the more complex it is to decrypt the ciphertext message without it, particularly using a "brute force" attack (Pfleeger, 1997, p. 113).

Encryption can be used to foil most attempts at compromising message security. If criminals cannot decrypt a message, then it is safe from being read or modified, even if it is intercepted. According to Pfleeger (1997), many encryption algorithms are *practically* unbreakable, and so are considered to be secure. This means that the time and resources required to break the key would be of more value than the data recovered, or that the data would no longer have intrinsic value after such time had passed. Many of these secure methods are in use today. However, as computers become faster, and with commensurate increases in connectivity, parallelism and the sophistication of cryptanalysis attacks, the length of key needed to maintain security is constantly increasing.

## 3.1. Conventional Encryption

Often called *single key, secret key* or *symmetric* encryption, *conventional* encryption is the most common and widely used form of encryption today (Alexander, 1996, p. 136). With this method, a plaintext message is encoded using an encryption algorithm and a key to produce a ciphertext message. Once the message reaches its destination, it is decoded using a decryption algorithm and the same key in order to retrieve the original plaintext message.

The most widely used conventional encryption algorithm is the Data Encryption Standard (DES) developed by IBM, and accepted by the US Federal Bureau of Standards in 1977 (Massey, 1992, p. 2). DES employs a combination of the traditional cryptographic methods of substitution, exchanging one symbol for another, and transposition, rearranging symbol positions. Individually these methods would be considered "weak" by modern cryptographic standards, but DES combines them in such a way that results in over 70 quadrillion possible transformation functions, making it very effective (Smid & Branstad, 1992, p. 54).

The biggest problem with this form of encryption is key management (Schneier, 1994, p. 140). Before the sender and receiver can exchange messages, somehow the key must first be transmitted between them. No matter how this is achieved, whether by phone, mail, fax or some other method, there is usually still a danger of interception. This is a large enough problem on a one to one basis, but consider the problem when there are hundreds, or even thousands of users who need to communicate in this manner. If even one copy of the key is compromised, then all communications amongst this user group are suddenly vulnerable.

## 3.2. Public Key Encryption

A second form of encryption, known as *public key* or *asymmetrical* encryption, offers a solution to the problem of key distribution (Stinson, 1995, p. 114). With this method, each user has a pair of mathematically related keys, each of which can be used to decrypt what the other has encrypted. One of the keys is kept as the owners' *private key*, which is kept secret, while the other, the *public key*, can be freely distributed to as many other users as desired. When a user wants to send a message to the owner of the key pair, they encrypt it using the public key, secure in the knowledge that the only key that will be able to decrypt the message is the corresponding private key owned by the intended recipient.

Obviously, this only provides secure communication in one direction. In order for a message to travel in the opposite direction the same process must be performed in reverse, thus requiring a second set of keys.

The most noticeable shortcoming of public key encryption is that because it is computationally expensive, it is significantly slower than conventional encryption (Till, 1997, [on-line]).

Diffie and Hellman (1976: a, b) were the first to reveal this method of encryption. However, it was in 1978 that Rivest, Shamir and Adleman developed the first concrete example of public key encryption (Davies & Price, 1989, p. 212), commonly called RSA after its creators. According to Schneier (1994), the RSA algorithm gets its security from the difficulty of factoring large numbers.

## 3.3. Specialised Techniques

The problem of being able to confidently associate a message with its supposed originator is a significant one for Electronic Commerce. In traditional face-to-face transactions, using a payment card for arguments sake, a merchant could always check that the card being used belonged to the person using it by comparing the signature given to the one on the back of the card. Obviously this is not possible when the transaction is an electronic one. So what's to stop a criminal in possession of someone else's payment card details pretending to be that person and purchasing goods? This type of fraud has had a significant impact on the popularity of Electronic Commerce to date, and is generally referred to as "spoofing".

The use of public key cryptography, in combination with digital signatures and digital certificates, discussed in Sections 3.3.1 and 3.3.2 respectively, provides authentication of messages and the individuals involved in electronic transactions.

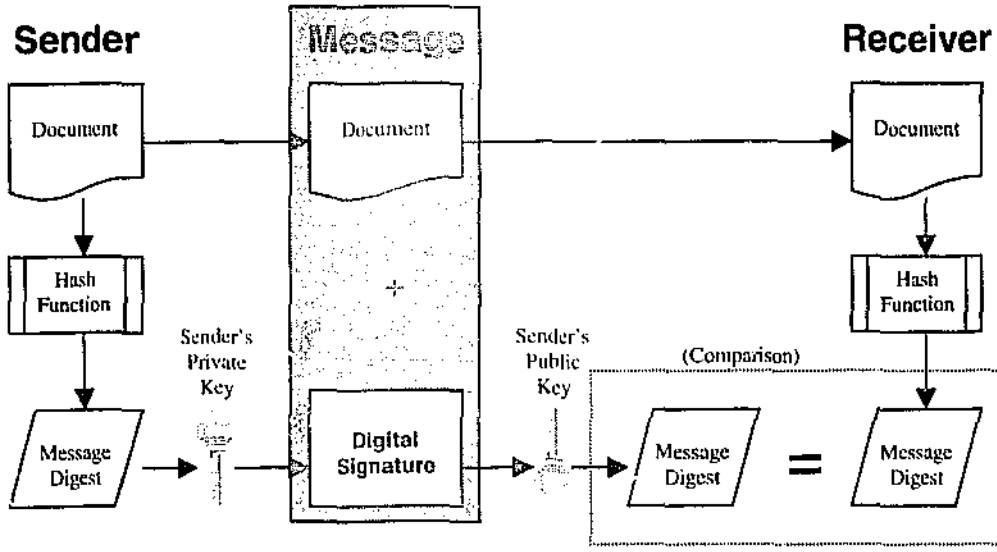
### 3.3.1. Digital Signatures and Message Digests

Assuming that it is possible for a sufficiently powerful or well informed adversary to intercept, decrypt, alter, and then re-encrypted a message while it is in transit between a sender and receiver, the receiver needs some method of ascertaining that the message received is in its original form. This can be achieved through the use of *message digests* and *digital signatures.*

A sender can generate a message digest of the original plaintext message or document by passing it through a one-way cryptographic hash function, i.e. one that cannot be reversed. When the message digest itself is encrypted using the sender's private key,

this is known as the *digital signature* of the message. This is then appended to the original message before transmission. The recipient of the message decrypts the digital signature and retrieves the message digest using the sender's public key, then generates the message digest of the plaintext message or document received using the public cryptographic hash function, and compares the two message digests for discrepancies. If there are no discrepancies, then the recipient knows that the message received is the one that was originally sent. The use of the sender's private key to encrypt the message digest provides proof of the origin of the digest, which in turn provides proof of the origin of the message itself (Ford & Baum, 1997, p. 112).

**Figure 1. Message Digests and Digital Signatures**




Of course, it should be noted that digital signatures by themselves do not guarantee non-repudiation. If a user's private key is conveniently "exposed" to the public, they can deny the authenticity of a particular message. Timestamps can partially help solve this problem by proving that a message was sent at a certain point in time, but this is hardly conclusive evidence of fraud. This problem has caused much discussion about the

possibility of sealing private keys in "tamper-resistant" modules, to stop such "accidental" exposure (Schneier, 1994, p. 36).

The message digest for any given message is unique. It is computationally infeasible for the same message digest to be generated by two different messages, as changing even a single bit in the original message will alter approximately half the bits in the resulting message digest. SHA is probably the most common hash function algorithm used to generate these digests as it is the primary hash function associated with the DSA (Ford & Baum, 1997, p. 221). See Section 3.3.2 for more information on the DSA.

Apart from the ability of cryptographic hash functions to provide authentication of the content and origin of messages, perhaps their most useful feature is that they generate a message digest of a predetermined size, regardless of the length of the original message or document. Message digests are only 160 bits in length if the Digital Signature Standard is used, which makes them a highly efficient way of signing lengthy messages (Ford, 1994, p. 84).

### 3.3.2. The Digital Signature Standard (DSS)

The National Institute of Standards and Technology (NIST) proposed the Digital Signature Standard (DSS) in August 1991. According to the Federal Register (cited in Schneier, 1994, p. 304):

> "A Federal Information Processing Standard (FIPS) for Digital Signature Standard (DSS).... specifies a public-key digital signature algorithm (DSA) appropriate for Federal digital signature applications.... considered during this

> process were the level of security provided, the ease of implementation... the ease of export from the U.S., the applicability of patents, impact on national security and law enforcement and the level of efficiency in both the signing and verification functions."

Despite a torrent of criticism and litigation, the DSS was eventually adopted as the federal standard for authenticating electronic documents on May 19th, 1994 ("What are DSA and DSS?", 1996, [on-line]) ("Digital Signatures", n.d., [on-line]).

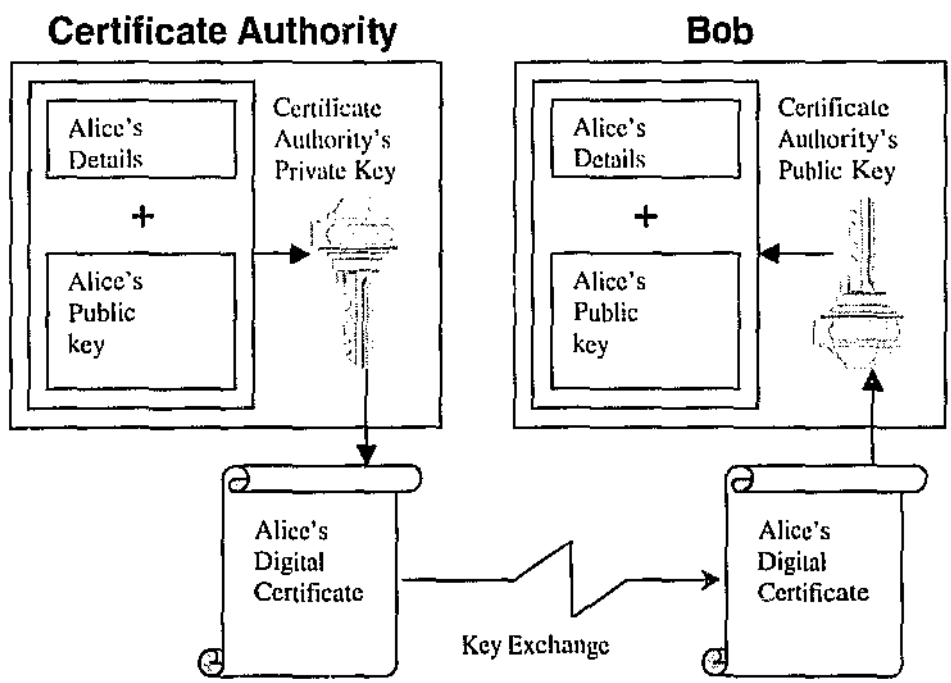
### 3.3.3. Digital Certificates

Although digital signatures do provide a way to verify that a message has not been tampered with since it was originally encrypted and sent, it still doesn't provide foolproof prevention of spoofing (Schneier, 1994, p. 36).

Before two parties can transact business electronically, they must be able to authenticate each other's identity. Before a merchant accepts a message from a consumer, they must be sure that the sender is who they say they are, and not an imposter using their own key pair. This requires that when the receiver obtains the senders public key, they must be able to confirm that the key belongs to the individual stated. This comes back then to the problem of secure key distribution. The option whereby the receiver obtains the senders public key in some other manner, e.g. registered mail, is not usually a practical solution between parties who may only interact once. The preferred method is to provide both the public key and some form of authentication by a trusted third party within the message itself (Ford & Baum, 1997, p. 193).

These trusted third parties are usually known as Certificate Authorities (CA). Once a CA has established the identity of an individual to their satisfaction, which is usually a fairly stringent process, they create a message that usually contains the individuals name and details, and their public key(s). This message is known as a *digital certificate*, and is signed with the CA's private key, meaning that it can be checked for authenticity by anyone using the CA's public key. Thus by including his or her digital certificate as part of an overall message a sender can simultaneously achieve authentication and key-exchange, i.e. provide proof of the identity and ownership of the public key (Ford & Baum, 1997, p. 194).

**Figure 2. Digital Certification**



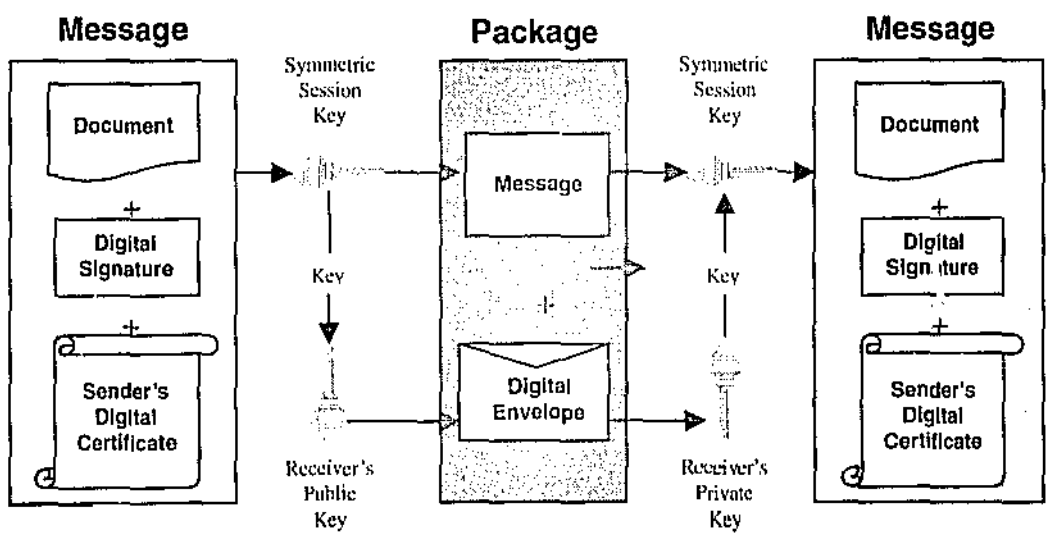

To get the maximum benefit from this scheme, it is desirable for as many people as possible to know the CA's public key. The more people who have access to this key, the greater the possible usage of the associated certificate. According to the SET

Business Description (1997), this allows for hierarchy with a high degree of trust, based on a single key (see Section 5.5).

### 3.3.4. Digital Envelopes

Usually, once all the various components of a message have been prepared, i.e. the actual plaintext message or document to be sent, the digital signature of the message or document, and the sender's digital certificate, the entire package is encrypted using conventional encryption prior to transmission. The symmetric key used for this is then encrypted using the receiver's public key and appended to the message. This encrypted key is called the *digital envelope*. This means that only the intended recipient can use their private key to "open" the digital envelope and obtain the symmetrical key to decrypt the rest of the message (SET Business Description, 1997, p. 21).

**Figure 3. Digital Envelopes**



## 3.4. Legal Issues

Despite the obvious usefulness of cryptography, many governments have grave concerns about the proliferation of such techniques when used in conjunction with the power of computers. In some countries this lead to cryptography and other dual-use technologies originally being classified in the same category as arms and other munitions for the purposes of import and export (Computer Technology Research Corp., 1996, p. 72).

The real difficulty lies in the fact that the Internet has largely broken down national boundaries. It is extremely difficult for countries to control the import and export of information in electronic form, and even if they do, the question of jurisdiction then raises it ugly head. The problems associated with crimes, or even misdirected transactions, which cross national boundaries are already well known (Watson, 1997, p. 52).

For the most part, officially, countries are concerned that if the use of "strong" cryptography becomes widespread, they will not be able to intercept or monitor electronic traffic concerning criminal activities. Of course, privacy activists are concerned that governments won't stop with known criminals, but will routinely monitor other traffic as well (Wisebrod, 1997, [on-line]).

One compromise solution to this problem is key escrow. This involves all cryptographic keys being kept in trust by a trusted third party. This would work in much the same way as wiretaps do. That is, if a government suspect someone of transmitting information associated with illegal activities, they can get a court order to

have the necessary key(s) released to allow them to monitor the transmissions. However, each time this method has been proposed, whether on a mandatory or voluntary basis, it has been rejected due to its perceived flaws and weaknesses (Abelson, Anderson, Bellovin, Benaloh, Blaze, Diffie, Gilmore, Neumann, Rivest, Schiller & Schneier, 1997, [on-line]).

Amongst others, these problems have lead to a number of international treaties that address this issue. Perhaps the most significant of these is the "Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies" (Broiles, 1997, [on-line]), which was ratified in July 1996, and was ultimately signed by 33 countries. Other significant organisations that have been working to develop guidelines include the European Union (EU), the Organisation for Economic Co-operation and Development (OECD), and the International Chamber of Commerce (ICC) (Koops, 1997, [on-line]).

### 3.4.1. Pertinent U.S. Legal Issues

As SET is being developed in the USA, and a large number of the companies initially proposing to develop SET compliant software are also in the USA, it is primarily this country's legislation that impacts upon its initial proliferation.

Control over the export of cryptography from the US was shifted from the International Traffic in Arms Regulations (ITAR) to the Export Administration Regulations (EAR) of the Department of Commerce at the end of 1996. This has resulted in a loosening of the export regulations where specific conditions apply. According to Koops (1997), the

new export rules distinguish between five categories of "encryption items" (EI) as follows:

1. Certain mass-market encryption software may be released from EI controls after a one-time review.

2. "Data recovery" crypto [cryptography] (meaning that government can access keys or plaintext with a lawful warrant) will be eligible for an export license to non-embargoed countries [embargoed countries currently include: Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan].

3. After a one-time review, (up to) 56-bit cryptography can be granted a six-month export license, provided the exporting business commits itself to incorporating a data recovery feature in its products within the next two years. This relaxation of controls will last until January 1, 1999: after two years, the export of non-recovery 56-bit cryptography will be prohibited again, and the same situation as before will hold (maximum 40-bit key length, with exceptions for financial institutions).

4. All other encryption items may be eligible for encryption licensing arrangements; items not authorized under a licensing arrangement will be considered on a case-by-case basis.

5. Encryption "technology" may be licensed for export on a case-by-case basis.

The US Department of Justice is also involved in the "case-by-case" decisions regarding export licenses.

The SET Business Description (1997) assures us that despite the restrictive regulations enforced by many nations concerning the import or export of cryptography, as a general rule these governments allow cryptography to be used when:

- The data being encrypted is of a financial nature;
- The content of the data is well-defined;
- The length of the data is limited; and
- The cryptography cannot easily be used for other purposes.

This is supported by the above summary of the EAR. With the gradual relaxing of export restrictions in regard to financial applications, it is apparent that even the governments acknowledge that Electronic Commerce can only flourish if the necessary software can be exported from the country of its origin.

# 4. The Current Defacto Standard

Although there are a number of secure transaction protocols currently vying for the title of Internet Standard, perhaps the most widely recognised of these is Netscape's Secure Sockets Layer (SSL). The SSL protocol is designed to provide a transport layer encryption scheme. The Internet Engineering Task Force (IETF) is currently reviewing the Internet Draft form of SSL version 3.0 to determine its suitability as such a standard. Of course in the final analysis, the key factor in determining whether or not something becomes a "standard" on the Internet is market consensus. If a product doesn't have support from both developers and users, then it is surely doomed to ultimate obsolescence. The current version of SSL, SSL version 2.0, already has the support of many of the industries major players, including IBM, Microsoft, and even Spyglass (Pompili, 1996, [on-line]), and many major developers now include support for SSL in their current applications.

This chapter provides a summary of the key security procedures and methods used by the SSL protocol to provide secure session connections between communicating parties.

## 4.1. Secure Sockets Layer (SSL)

SSL can be used to secure nearly everything that's transmitted between a browser and a server, from passwords and logon IDs to files being downloaded from an FTP server (Pompili, 1996, [on-line]).

According to Freier, Karlton & Kocher (1996), apart from the primary goal of providing privacy and reliability between communicating applications, the goals of SSL Protocol, in order of their priority, are:

1. Cryptographic security - SSL should be used to establish a secure connection between two parties.

2. Interoperability - Independent programmers should be able to develop applications utilising SSL 3.0 that will then be able to successfully exchange cryptographic parameters without knowledge of one another's code. However, it is not the case that all instances of SSL (even in the same application domain) will be able to successfully connect. For instance, if the server supports a particular hardware token, and the client does not have access to such a token, then the connection will not succeed.

3. Extensibility - SSL seeks to provide a framework into which new public key and bulk encryption methods can be incorporated as necessary. This will accomplish two sub-goals: to prevent the need to create a new protocol (and risking the introduction of possible new weaknesses) and to avoid the need to implement an entire new security library.

4. Relative efficiency - Cryptographic operations tend to be highly CPU intensive, particularly public key operations. For this reason, the SSL protocol has incorporated an optional session caching scheme to reduce the number of

connections that need to be established from scratch. Additionally, care has been taken to reduce network activity.

The SSL protocol is comprised of two basic layers; the SSL Record Protocol, which sits at the lowest level acting as an intermediary between the transport protocol, e.g. TCP/IP, and the higher level protocols themselves, like the Handshake Protocol. The SSL Record Protocol is used for encapsulation of the various higher level protocols. This allows SSL to provide a transparent security layer between the network itself, and a variety of network service protocols such as Hypertext Transfer Protocol (HTTP), Telnet, Network News Transfer Protocol (NNTP), and File Transfer Protocol (FTP) ("Secure Sockets Layer", 1997, [on-line]).

### 4.1.1. SSL Connections

According to Freier, Karlton & Kocher (1996), the SSL Handshake Protocol is designed to allow a server and a client to authenticate each other, and to negotiate cryptographic details such as algorithm, Machine Access Code (MAC) secrets, and keys before any data is exchanged between applications. This provides connection security that has three basic properties:

1. The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for [bulk] data encryption (e.g. Data Encryption Standard, etc. (See Chapter 3))

2. The peer's identity can be authenticated using public key cryptography (e.g. RSA, DSS, etc. (See Chapter 3)).

3. The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g. SHA, MD5, etc. (See Chapter 3)) are used for MAC computations.

SSL takes the data to be transmitted, breaks it into manageable blocks of a predetermined size, then generates a MAC for each block, and encrypts and transmits each block and MAC together. Data blocks that are smaller than the agreed size are padded with some regular pattern, usually all zeros. Before the MAC is calculated, SSL also provides the option of compressing the data. Consequently, when the data is received at the other end, it is decrypted, verified, decompressed if necessary, and then reassembled.

### 4.1.2. Client/Server Authentication

Client and server authentication is optional in SSL. When a client initiates communication with a server, the initial message exchange is used to establish some or all of the following:

- The SSL protocol version,
- A unique Session ID,
- The cryptographic suite to be used, and
- The compression method.

In the initial response from the server, it may supply a certificate to provide authentication, and likewise it may request one in return. These certificates can be digitally signed if required. If an appropriate certificate is not available, the server will

respond by initiating a public key exchange with the client. The client responds using the new key(s) and algorithms to establish the final parameters for the session.

Once the client and server have exchanged public and secret keys, and established a secure connection, they can begin exchanging data using the agreed upon methods.

### 4.1.3. Message Authentication

SSL uses a Message Authentication Code (MAC) to verify the integrity of messages. A MAC is basically a message digest, as described in Section 3.3.1. Although SSL can make use of a number of possible hashing algorithms including SHA and MD5, it is most likely that SHA would be used predominantly, as it is generally considered stronger than most others, and generates a 160 bit digest (Ford, 1994, p. 84), making it compatible with the Digital Signature Algorithm (DSA).

## 4.2. Summary

This Chapter describes the SSL security protocol, the current defacto standard for the Internet. As was observed at the beginning, SSL has much backing from major companies involved with Internet development, which means that it is likely to maintain a significant presence for the foreseeable future at least. When used to full effect it fulfils its objectives of privacy and authenticity through the use of encryption and digital certificates (Reid, 1996, p. 667). However, a number of obstacles exist that must be overcome if SSL is to receive universal acceptance as an industry standard (Reid, 1996, p. 667). One such problem is the difficulty in exporting software that employs such a generic encryption scheme from the US, due to that countries restrictive policy on such export.

Chapter 5 introduces the SET protocol, which is currently vying with SSL for widespread acceptance as the standard security protocol for Electronic Commerce.

# 5. Secure Electronic Transaction (SET) Protocol

In order to maintain as much accuracy as possible, the information in this chapter is sourced almost exclusively from the SET Business Description (1997).

## 5.1. Introduction

The SET specification defines protocols that are aimed at providing authentication for all parties involved in an electronic transaction, while at the same time ensuring the integrity and confidentiality of all information transmitted.

It seems obvious that most payment card brands should have a vested interest in supporting the development of secure transaction standards for a number of reasons. The development of an appropriate standard, during what is effectively the infancy of Electronic Commerce, will probably save great expense and difficulty later by avoiding having to reconcile different systems that may have been developed otherwise. Additionally, such standards will help preserve the integrity of all parties involved in such transactions, which should increase consumer confidence in privacy and security, decrease the amount of payment card fraud, and generally accelerate the growth of a potentially huge marketplace.

The SET specifications have been carefully designed to ensure that they possess the maximum appeal for software vendors, financial institutions and consumers alike. This has been achieved in a number of ways. While the SET protocols define an open payment card standard, based on existing standards where possible, it is also documented in a manner that will allow software vendors to develop globally

interoperative software, which can be implemented across many different combinations of hardware and software. SET implementations will "bolt-on" to existing client applications, minimising the impact that they will have on the current commercial systems and infrastructure. One of the key aims of SET, designed to gain it the support of the financial sector, is to provide an efficient set of protocols for acquirers and card-issuing banks. In short, SET is designed to be easy for everyone to use and/or implement, while causing minimal disruption to current systems in the process.

At present, vendors who develop SET compliant applications must submit them to independent testing by Tenth-Mountain-Systems, Inc.. However, these tests only certify compliance against the SET Draft Reference Implementation version 0.0. This is a temporary measure until a long-term SET Compliance Authority (SCA) can be set up to test compliance with version 1.0 ("Compliance", 1997, [on-line]).

The key requirements of the SET protocols, as defined within the SET specification documents, are as follows:

- Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
- Ensure the integrity of all transmitted data.
- Provide authentication that a cardholder is a legitimate user of a branded payment card account.
- Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.

- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an Electronic Commerce transaction.
- Create a protocol that neither depends on transport security mechanisms nor prevents their use.
- Facilitate and encourage interoperability among software and network providers.

The following discussion broadly outlines the key issues.

### 5.1.1. Confidentiality of Information

In order for Electronic Commerce using payment card products to be a success, cardholders must be confident that all information that they commit to such transactions will be completely secure during transmission, and will only be recoverable by the intended recipient. The SET protocols achieve this through the use of message encryption, using a combination of conventional (DES) and public-key (RSA) encryption (See Chapter 3).

### 5.1.2. Integrity of Data

Data that is transmitted must be guaranteed against deliberate or accidental alteration whilst in transit. The integrity of all information transmitted using SET is validated through the use of digital signatures.

In most cases, the SET specifications require that the primary participants in a transaction have two pairs of keys, a "signature" pair, used for the creation of digital signatures, and a "key-exchange" pair, used for general encryption/decryption purposes

(See Chapter 3). The exception to this rule is the cardholder, who under normal conditions does not necessarily require a key-exchange pair (see Section 5.4).

### 5.1.3. Cardholder Account and Merchant Authentication

Because of the anonymous nature of Electronic Commerce, cardholders and merchants cannot physically identify those with whom they are dealing. There is a requirement for some method by which all parties can give proof of identity. Merchants must be assured that an individual trying to make a purchase is the legal holder of the card being used. Likewise, cardholders want assurance that the business they are about to make payment to is a valid merchant.

SET uses a combination of Cardholder Certificates and Merchant Certificates to achieve such identification, and to provide non-repudiation (See Section 3.3.3).

### 5.1.4. Interoperability

The SET specifications have ensured that they support a wide range of hardware and software platforms through the use of specific protocols and message formats. This means that there will be no requirement for cardholders and merchants to use the same hardware and software platforms, beyond the obvious requirement that all software will need to be compliant with the SET standard.

## 5.2. Participants

Electronic Commerce on the Internet using payment cards involves the traditional participants, being the card-issuing institution, Acquirer, cardholder and merchant, but can also involve payment gateways and third parties. This Section describes these terms, and their significance in SET transactions.

### 5.2.1. Issuers

Payment card issuing institutions (Issuers) guarantee payment for authorised transactions using their products. This is dependent on the product being used in accordance with both the agreed terms and conditions, and with domestic legislation. Although the Issuer is responsible for all debts if a cardholder uses credit and then cannot or will not pay back the moneys owed, in the case of disputed transactions the onus of proof often falls squarely on the merchant (Till, 1997, [on-line]).

### 5.2.2. Acquirers

Acquirers are the financial institutions that process payment card transactions for the merchants. The acquirer purchases the credit transaction from the merchant, immediately crediting the merchants account for the amount of the transaction minus the discount. The discount is a combination of the charge that the Issuer will deduct from the transaction for processing, known as interchange reimbursement fees, plus the Acquirers own percentage profit (Till, 1997, [on-line]).

### 5.2.3. Cardholders

For the purpose of Electronic Commerce, a cardholder can include any individual or organisation that has been issued a payment card of any type by an Issuer. SET does not differentiate between card types, or transaction types, as it acts purely as a "front-end" to such transactions.

### 5.2.4. Brands

There are a number of different types of payment cards available today. Financial institutions like banks offer a variety of credit and debit card products. Other

institutions that provide financial services often offer their own unique products, which they promote themselves, e.g. retail chain cards, like Australia's MyerCard. In the case of these types of products, the Issuer often also acts as the Acquirer for relevant transactions.

### 5.2.5. Merchants

As with more mundane forms of commerce, a merchant on the Internet offers to sell or provide goods and/or services. An Internet merchant who accepts payment cards of any type must have a relationship with an Acquirer who can process such payments. Transactions of this type have been deemed to fall into the same category as Mail Order/ Telephone Order (MOTO) transactions, making them far more expensive for merchants to process than EFTPOS (Till, 1997, [on-line]).

### 5.2.6. Payment Gateways

According to the SET Business Description (1997), "A payment gateway is a device operated by an Acquirer or a designated third party that processes merchant payment messages, including payment instructions from cardholders." Obviously, because such gateways are designated to handle sensitive financial data, and therefore must be known to be trustworthy, they must be certified like all other parties.

### 5.2.7. Third Parties

Third parties may sometimes be nominated by Issuers and Acquirers to handle the processing of payment card transactions. However, as this does not change the functionality of such transactions, SET does not differentiate between these processors.

## 5.3. Scope

Although the entire Internet shopping experience begins at the point where a consumer first becomes aware of a merchant of interest to him/her, the SET specifications are only concerned with the transaction from the point at which financial information begins to be exchanged. SET is designed to protect such information while it is being used in the tripartite relationship between the cardholder, the merchant, and the Acquirer. This covers a number of steps including; the cardholder sending an order, complete with payment details, the merchant requesting and receiving payment authorisation from the Acquirer, and then sending an order confirmation back to the cardholder.

The SET Business Description (1997) identifies the following lists pertaining to the overall scope of the SET specifications.

Within the scope:

- Application of cryptographic algorithms (such as RSA and DES)
- Certificate message and object formats
- Purchase messages and object formats
- Authorization messages and object formats
- Capture messages and object formats
- Message protocols between participants

Outside the scope:

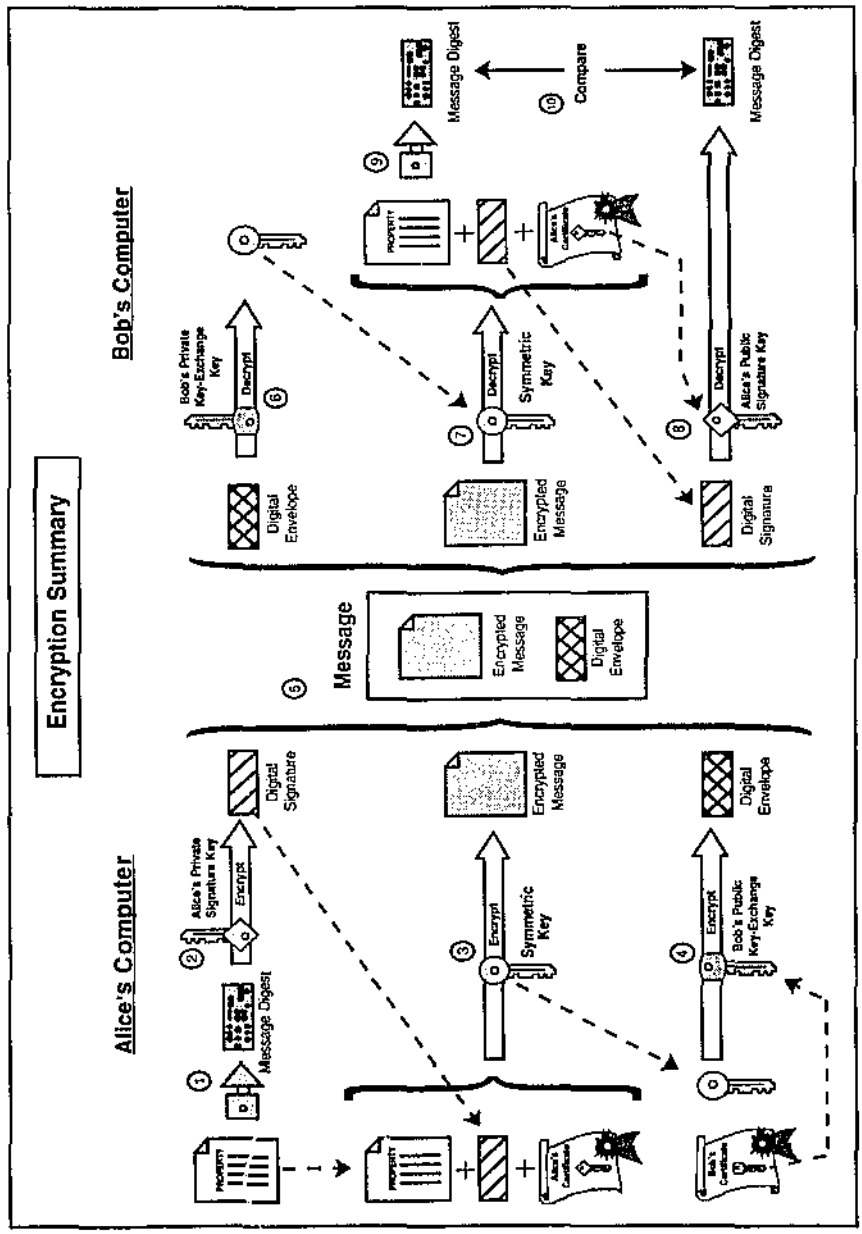
- Message protocols for offers, shopping, delivery of goods, etc.
- Operational issues such as the criteria set by individual financial institutions for the issuance of cardholder and merchant certificates
- Screen formats including the content, presentation and layout of order entry forms as defined by each merchant
- General payments beyond the domain of payment cards
- Security of data on cardholder, merchant, and payment gateway systems including protection from viruses, Trojan horse programs, and hackers
- The means by which financial institutions authenticate cardholders and merchants

It should be noted that this is only a partial list of categories of things that are outside the scope of the SET specification.

## 5.4. Encryption

The following diagram illustrates the complete encryption process used by the SET specifications for the transmission of a secure message between a sender (Alice) and receiver (Bob).

**Figure 4. SET Encryption Summary**




**(SET Business Description, 1997, p. 20)**

The steps involved in this process can be summarised as follows:

1. The *message digest* of the document to be sent is computed using a public one-way cryptographic hash function.

2. Alice then signs the *message digest* with her *private signature key* in order to create the *digital signature* of the document.

3. The document to be sent, the *digital signature*, and Alice's *signature certificate*, containing her *public signature key*, are all encrypted using a randomly generated symmetric *session key* to form the final *message*.

4. The symmetric *session key* is then encrypted using Bob's *public key-exchange key*, obtained from his *key-exchange certificate*, to form the *digital envelope*.

5. The encrypted *message* and the *digital envelope* are then both sent to Bob.

6. Bob decrypts the *digital envelope* using his *private key-exchange key* in order to retrieve the *session key*.

7. The *session key* is then used to decrypt the *message*.

8. The *digital signature* contained in the *message* is decrypted using Alice's *public signature key*, obtained from her *signature certificate*, to obtain the original *message digest*.

9. The same public one-way cryptographic hash function is used to generate a new *message digest* of the actual document received.

10. Bob then compares the original *message digest* to the new *message digest*. If they are identical then the message has not been altered since it was first sent.

This process clearly illustrates the need for each participant to have key/certificate sets for both key-exchange and the creation of digital signatures.

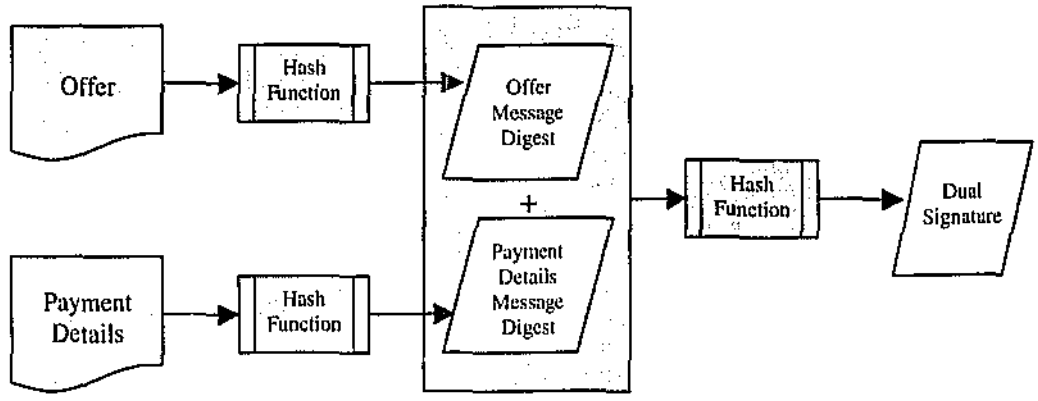
### 5.4.1. Dual Signatures

Dual signatures are a new application of digital signatures introduced in the SET specification. The concept evolved from the need to protect information from different parties in a given transaction. For example, if Alice wanted to make an offer to purchase some goods from Bob, she would send him the offer and the payment authorisation for use if the offer is accepted. Obviously, Alice only wants the funds transferred if the offer is accepted. Furthermore, Alice doesn't want the bank to see the terms of the offer, and she doesn't want Bob to see her payment information. All of this can be achieved by linking the offer and the payment details with a dual signature.

Computing the message digests of each separate message, in this case the offer and the payment information, concatenating the two digests and then computing the message

digest of the result and signing it with the sender's private signature key generates a dual signature. This dual signature, along with the message digest of *both* messages is included in each message to allow verification.

**Figure 5. Dual Signatures**

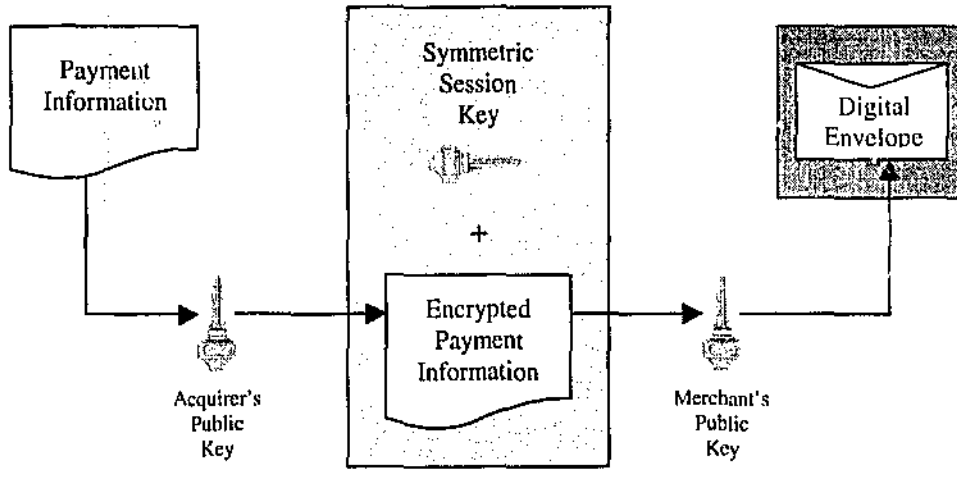



For example, Bob's message would include the offer, the message digest of the offer, the message digest of the payment information, and the dual signature. The offer itself can be authenticated as was described in the previous section. If Bob concatenates the message digest of the offer received and the message digest of the payment information, then generates the message digest of the result, he can compare that against the decrypted dual signature to verify its authenticity. Once Bob notifies the bank of his acceptance of the offer, such notification including a message digest of the offer being accepted, the bank can verify its message in the same manner, thus ensuring that the offer being accepted is the one that Alice authorised payment for. Neither Bob nor the bank gets to see the details sent to the other.

SET uses dual signatures to link orders sent to merchants with payment information destined for the merchants Acquirer. When a merchant requests authorisation for payment, the message to the Acquirer includes the encrypted payment information received from the cardholder, and the message digest of the order received, thus allowing the Acquirer to verify the dual signature.

The one key difference between a standard message to a merchant, and payment information destined for the Acquirer, is that the payment information itself is actually included in the digital envelope, encrypted with the Acquirer's public key-exchange key. This provides payment information with the additional protection of public key cryptography.

**Figure 6. SET Payment Information**



### 5.4.2. Export Issues

Because the SET protocols are only concerned with the "shopping" side of Electronic Commerce, and have clearly defined the use of encryption to financial transactions of this nature only, many of the concerns of governments regarding the export of technology that utilises encryption have been alleviated. Despite the difficulties associated with the export of this type of technology, the SET Business Description (1997) assures us that providing software vendors planning to use the SET protocols can demonstrate that the cryptography used can not be easily put to other purposes, export licenses should be obtainable.

Of course this is yet to be put to the test in many of the nations hostile to the use of cryptography.

## 5.5. Certificates

As was discussed above, digital certificates are used to significantly strengthen authentication procedures. In addition to the standard information contained in digital certificates, SET certificates also provide information specific to electronic payment card transactions. Each participant requires a certificate appropriate to the role that they play in such transactions, i.e. cardholder, merchant, Acquirer, etc. This requires that a number of separate CAs are used to issue these certificates, each having a specialisation in one of the required areas. The "hierarchy of trust" that SET uses for certificate issuance is described in Section 5.5.1.

According to Till (1997), the system for issuing digital certificates under the SET regime may take some time to establish. In the interim it is likely that banks will make use of existing private CA's like VeriSign and GTE CyberTrust.

It should be noted that because most SET transaction participants require both key-exchange and signature key pairs, they also require two digital certificates in order to authenticate both sets. The CA can create both of these certificates at the same time.

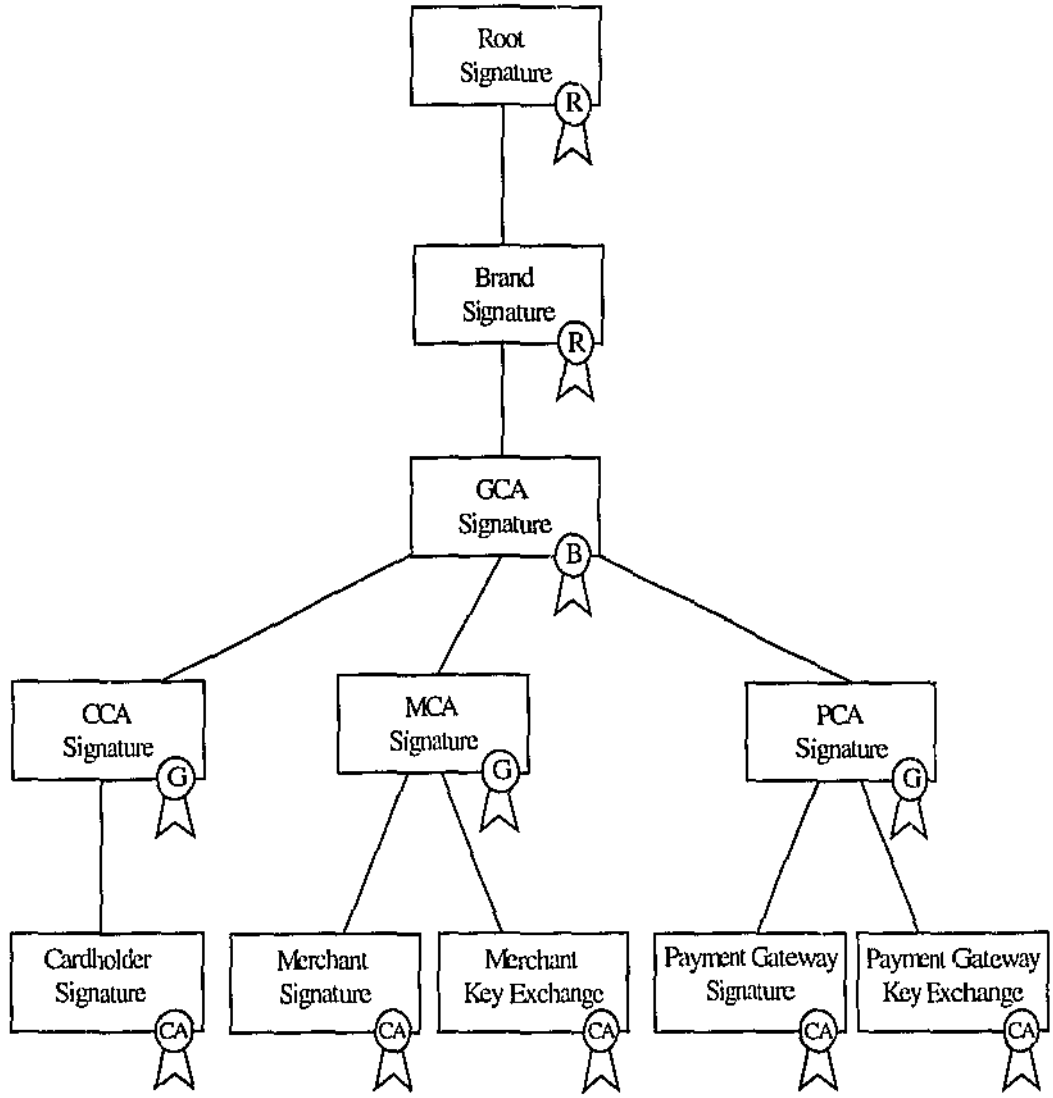
### 5.5.1. Hierarchy of Trust

According to the SET Business Description (1997):

> "SET certificates are verified through a hierarchy of trust. Each certificate is linked to the signature certificate of the entity that digitally signed it. By following the trust tree to a known trusted party, one can be assured that the certificate is valid. For example, a cardholder certificate is linked to the certificate of the Issuer (or the Brand on behalf of the Issuer). The Issuer's certificate is linked back to a root key through the Brand's certificate. The public signature key of the root is known to all SET software and may be used to verify each of the certificates in turn."

The following diagram illustrates one possible hierarchy of trust, but this may be altered in a number of ways. For example, each payment card brand may not necessarily operate a Geopolitical Certificate Authority (GCA), which is merely an optional intermediate national CA for each country or political region, between itself and the other various Certificate Authorities.

**Figure 7. SET Hierarchy of Trust**




**(SET Business Description, 1997, p. 26)**

The "ribbons" in the above diagram indicate which Certificate Authority signed each certificate.

### 5.5.2. Cardholder Certificates

SET cardholder certificates are the electronic equivalent of an actual payment card. These certificates are signed by a financial institution, and consequently can only be

issued by a financial institution. Such certificates are only issued with the approval of the cardholders Issuer.

Cardholder certificates do not actually contain the payment card account information, but rather are the equivalent of a message digest created by running both the account information and a secret value through a one-way cryptographic hash function. This secret value is known only to the cardholder's software, and is included with the encrypted payment information. If the account information, i.e. card number, expiry date, etc., and the secret value are known, then the link to the certificate can be proven. In a normal transaction, the cardholder certificate is transmitted to merchants with purchase requests and encrypted payment details. This is then passed along to the Payment Gateway or Acquirer to provide proof of ownership of the card by the cardholder. A merchant can observe none of this information by looking at the certificate, but can be assured at least that if the Acquirer confirms payment then the link has been verified.

When a cardholder applies for a certificate they are indicating their intention to participate in this type of Electronic Commerce. Under the current specification Issuers are under no obligation to grant the certificate application. Indeed, in version 1.0 of the SET specifications, it is not even a requirement that Issuers use cardholder certificates at all, although failure to do so would significantly weaken the SET authentication process. The reason behind this optional exclusion appears to be in order to allow vendors to initially develop SET compliant software without the requirement of an existing SET compliant certificate authority hierarchy.

### 5.5.3. Merchant Certificates

Merchant certificates indicate to consumers that they are authorised by an Acquirer to accept payment cards of a particular brand. Merchants must have a separate set of certificates for each brand of payment card, as each certificate originates from the Payment Brand CA in the SET "hierarchy of trust".

Like cardholder certificates, because merchant certificates are signed by the merchant's financial institution, they can only be issued by a financial institution, and cannot be alter by a third party.

### 5.5.4. Gateway Certificates

Because Acquirers or their designated Payment Gateways are trusted to process the cardholder's payment details, they have to be certified by the cardholder's payment brand. These certificates authorise the Payment Gateway to process payment authorisations, the request from a merchant for authorisation of an individual transaction, and capture messages, the request from a merchant for payment.

The cardholder receives a copy of this certificate in order to obtain the public key necessary to encrypt their payment details, such that nobody other than the Acquirer or Payment Gateway can access them.

### 5.5.5. Acquirer Certificates

Like all participants in a SET transaction, Acquirers must be certified. However, Acquirers who also wish to be Certificate Authorities, i.e. issue certificates to merchants

on behalf of a particular payment card brand, must in turn be certified by that same payment card brand.

This is not essential, as the Acquirer can instead opt to pass such request on to the payment card brand for processing.

### 5.5.6. Issuer Certificates

Issuers can likewise opt to be a Certificate Authority in order to issue certificates to cardholders. As with Acquirers, this requires that they in turn be certified by the payment card brand.

Issuers may also opt not to be a CA, and to pass all such requests on to the payment card brand for processing.

### 5.5.7. Root Key

The root key is the primary building block of the SET certificate hierarchy, or indeed any certificate hierarchy, as it is with this key that the authenticity of any certificate is ultimately verified. Consequently, the security and integrity of the root key is of paramount importance.

The root key is available to software vendors to include with any SET compliant software they develop. It is distributed in a self-signed certificate, which can be validated by sending a hash of the certificate to the originating Certificate Authority. In the rare case that a vendor has an invalid root certificate, the Certificate Authority will respond by sending a valid copy of the root certificate in the response.

When a root key is generated, a replacement root key is also generated. This replacement key is the next descendant of the current key, i.e. will be used to replace it when required. A hash of the replacement root key and the self-signed certificate of the current root key are distributed together.

When the root key is to be replaced, SET software is notified by the delivery of a self-signed certificate containing the new root key, and a hash of the new replacement key. The new root key is verified by calculating its hash and comparing it to the previous replacement root key hash.

## 5.6. Limitations

The SET specification documents clearly state that only transactions involving payment cards are within their scope. Despite the many strengths of the SET protocols, this appears to be the one possible weakness in the overall approach that is being adopted in the construction and marketing of the specifications. To understand why this is a problem, the usefulness of payment cards on the Internet needs to be evaluated.

### 5.6.1. Advantages

Because most payment card brands are supported by a large number of financial institutions, they represent a payment system that should be able to cope for the foreseeable future with the constantly increasing number of users of Electronic Commerce. This does presuppose the fairly immanent establishment of a broad payment infrastructure. However, with inception of co-operative efforts like EDS ReadySET ("EDS, HP and VeriFone Team to Lower Costs and Simplify Operation of

Internet Processing Services for Banks and Financial Institutions", 1997, [on-line]), a global payment infrastructure available to all banks, this should be achievable.

The use of dual signatures in SET assures cardholders that they will have the maximum possible privacy of information when using payment cards. Not only will the banks get no more information about transactions than they already do with current systems, but merchants will no longer get any card details whatsoever. This segregation of information should prevent any unwanted additional analysis of individual spending patterns, while at the same time providing reasonable auditability.

One of the most significant advantages of payment cards is the enormous existing customer base. Payment cards are already possessed by many millions of people, major brands are accepted by nearly every business, and the vast majority of financial institutions already have the infrastructure to process such transactions. Because of this broad base of support, this also means that payment cards represent a fairly reliable form of payment. Ultimately, the number of payment gateways that will support payment card transactions should be large enough that if one server is unavailable, an alternate server should be available to replace it temporarily without too much difficulty. Although not stated specifically, it appears that the issue of availability of service is outside the scope of the current SET specifications. The possibility of "Denial of Service" attacks is deemed to be within the problem domain of a secure payment processing infrastructure, rather than related to individual transactions.

### 5.6.2. Disadvantages

Payment cards in general have a serious limitation for some Internet transactions. It is likely that the Internet is going to spawn a variety of "micropayments", probably in the order of a few cents, required for such things as royalty payments on information, music, etc. The transaction charges attached to most payment cards, and the size and speed of the SET transactions used to process them, make them inefficient for such small payments.

Additionally, as payment card transactions are currently classified as Mail Order/ Telephone Order (MOTO) transactions, and as such attract much higher charges than face-to-face payment card transactions, businesses are less likely to accept this form of payment for relatively small amounts (Till, 1997, [on-line]).

## 5.7. Summary

This Chapter described the structure and security features offered by the SET protocols, which when employed fully for Electronic Commerce transactions will provide:

- Effective authentication of all parties in a transaction, including verification of their authority to participate using specific payment card brands,
- Easily verifiable digital certificates based on a purpose-specific hierarchy of trust,
- Secure and verifiable transmission of data,
- Privacy of payment information, and
- Non-repudiation of transactions.

Chapter 6 compares SET and SSL to determine their relative effectiveness, and investigates the comparative strengths and weaknesses of the protocols in providing secure transactions for Electronic Commerce.

# 6. Comparing SET and SSL

As was discussed in Chapter 2, the fundamental requirements of a commercial electronic transaction can be summarised as follows:

- Strong authentication of the identity and authority of all parties,
- Compatibility of payment method,
- Security of payment information at receiving end,
- Security of all information in transit against alteration, deletion or modification, and
- Non-repudiation for all parties.

## 6.1. Authentication

The need for fairly airtight authentication is obvious. Without it neither party can be sure of with whom they are dealing, or whether they have the authority to perform the transaction. The key tools used to provide authentication are digital signatures and digital certificates.

### 6.1.1. SET

SET provides strong authentication through the use of digital certificates issued from a purpose specific Root CA.

These certificates are virtually impossible to forge, as they must be created using a succession of signatures starting with the root key, which is known only to authorised developers and CAs. Likewise, an earlier recipient cannot reuse them to impersonate a

particular party. For example, a cardholder's certificate cannot be reused in future transactions, as the secret value needed to authenticate the link to the certificate is known only to the cardholder's software. Similarly, merchant key-exchange and signature certificates are useless to third parties, as they would not possess the corresponding private keys.

Although normally considered weak when used alone (see Section 3.3.1), the additional authentication offered by the use of digital signatures under SET is significant, as the SET signature certificate provides confirmation of the link between a cardholder and a payment card.

### 6.1.2. SSL

According to Freier, Karlton & Kocher (1996), SSL provides three distinct possible levels of authentication: authentication of both parties, server authentication with an unauthenticated client, and total anonymity. As can be observed from this, the use of certificates for authentication under SSL is optional. However, even assuming that in the case of Electronic Commerce certificates would be mandatory, SSL only uses such certificates to identify the server and the "client". No connection between the client and the payment method being offered is verified. Potentially this opens the way for payment card fraud if individual card details are compromised.

Additionally, the SSL protocol uses X.509 digital certificates, which presents a problem with widespread key distribution and authentication due to the poor uptake of the X.500 directory services (Reid, 1996, p. 667).

## 6.2. Compatibility

Before a cardholder provides a vendor with their payment card details, they want to be sure that the merchant in question is authorised to accept that form of payment. Likewise, the merchant needs to confirm that the client is the legitimate holder of the payment card being offered.

### 6.2.1. SET

Once again SET achieves this through the use of certificates. SET certificates provide confirmation of the relationship between a cardholder and the payment card being used (currently optional, see Section 5.5.2), and evidence of a merchants identity and confirmation of their authority to accept transactions using a given payment card brand.

All certificates issued by the SET "hierarchy of trust" stem from the payment brand (see Section 5.5.3), thus ensuring that the party in question is authorised to accept or use that type of payment card. For consumers, this provides similar authentication to the decal displayed in an ordinary shop window, only with greater surety.

### 6.2.2. SSL

Because SSL was not designed specifically for Electronic Commerce, it provides no standard mechanism for this kind of authentication.

## 6.3. Payment Security

One big issue in the use of payment cards at any level, electronic or otherwise, is the privacy of the card details. Merchant fraud, i.e. merchants abusing payment card information that has come into their possession through a prior transaction, currently

accounts for approximately one third of payment card fraud (Computer Technology Research Corp., 1996, p. 133).

### 6.3.1. SET

SET provides for the elimination of merchant fraud through the use of dual signatures. This means that merchants never gain possession of payment cards details. Instead they merely receive verification of the details and card ownership from the Acquirer.

### 6.3.2. SSL

The SSL protocol is merely designed to set up a secure session between a client and server. In the case of Electronic Commerce this means the consumer and merchant. There is no provision in SSL specifically for the processing of financial transactions of this nature. Payment card details are sent to the merchant, who then processes them as they would in a normal MOTO transaction.

## 6.4. Information Integrity

Electronic Commerce requires that all financial information transmitted be secured during transmission against accidental or deliberate alteration or interception.

### 6.4.1. SET

The cryptographic techniques used by SET are considered amply strong to thwart the current level of possible cryptanalysis attacks ("Just How Strong is RSA in SET?", 1997, [on-line]). SET uses 1024-bit public key encryption (RSA), and 56-bit conventional encryption (DES). Although this level of DES encryption has proven breakable with modern cryptanalysis techniques (Ford & Baum, 1997, p. 104) (Pompili, 1996, [on-line]), the SET protocol's use of dual signatures and digital envelopes mean

that payment card details are also encrypted using RSA (see Section 5.4.1). Effectively this means that even if an attacker succeeded in breaking the conventional encryption used to encrypt the bulk of a message, the payment information would still be protected.

The use of digital signatures by the SET protocols ensures that the integrity of all information transmitted can be verified by the recipient.

### 6.4.2. SSL

SSL only uses public key encryption and digital signatures during the initial "handshake" phase of a session. Thereafter it relies upon conventional encryption, combined with keyed MACs, to protect and verify the integrity of data (see Section 4.1.1). The length of keys allowed under SSL varies depending on whether you are in the US or not. Because an SSL session can be used for any type of transmission, not just financial, its export is controlled by the Export Administration Regulations of the US Department of Commerce (see Section 3.4.1).

According to the Netscape Policy on Encryption Export (1997), current US legislation only allows the export of SSL versions that use a maximum 40-bit conventional encryption key. Netscape itself admits that this is inadequate for high levels of security. Indeed, the current version of SSL has already been cracked at least once (Pompili, 1996, [on-line]).

Versions of SSL available within the US are far stronger, but as Electronic Commerce is already a global issue, this is of small comfort to consumers in general.

## 6.5. Non-repudiation

Both consumers and merchants alike need some assurance that the other party involved in a transaction is going to fulfill their part in the exchange. Consumers don't want to make payment and then not receive what they paid for, and merchants don't want consumers disputing the payment after the goods or services have been delivered. Both parties need a method of proving the others agreement to the original transaction.

The use of public key cryptography provides a minimal level of non-repudiation. However, as was discussed earlier, this does not stop someone from fraudulently claiming that his or her private key was compromised and used by an unknown third party.

### 6.5.1. SET

Through the combined use of digital signatures, key-exchange certificates, and signature certificates, SET effectively eliminates the possibility that either party in a transaction could viably repudiate a transaction. In many countries, including Australia, digital certificates are now admissible under the Laws of Evidence as proof of identity.

### 6.5.2. SSL

Assuming that an SSL session was established using digital certificates to authenticate both parties, and that a reliable CA issued the certificates in the first place, then SSL provides a reasonable level of non-repudiation.

## 6.6. Summary

In fairness, it should be noted that SSL is a general protocol for securing network transmissions, and was not designed for Electronic Commerce specifically. However, the conclusions seem fairly self-evident; the SET protocol, which was designed specifically for Electronic Commerce transactions, offers many clear advantages over SSL when used for this purpose.

Both SET and SSL can provide authentication through the use of digital certificates and digital signatures, but only SET can provide a positive link between the parties in the transaction and a specific payment card brand.

Both protocols provide reasonable message security and integrity through the use of encryption techniques. However, the use of dual signatures in SET provides for significantly higher protection of payment information. There is little doubt that SSL is less resource intensive than SET given its reliance on conventional cryptography to perform the bulk of the encryption load. However, the strength of the encryption employed in the international version of SSL, that is the version released for export from the US (see Section 6.4.2) is significantly weaker than that employed by SET.

Finally, both protocols use certificates that provide a level of non-repudiation. However, the use of multiple key/certificate pairs in SET provides additional proof of participation.

Of course, no system is one hundred percent foolproof (if it is, someone just invents a better fool), but it appears that when performing electronic transactions using SET, the only weak link is the users. If someone who knew a users password(s) and payment card details were to gain access to that users computer, then they would conceivably be able to impersonate them. However, this scenario is unlikely to present itself where any remotely responsible user is concerned. This may be especially true in future, as it is likely that smart cards will eventually be used to store sensitive information such as digital certificates. This will allow users to carry their digital certificates and secret values around in their pocket, providing greater mobility and additional security to the overall scheme.

# 7. Conclusions

The previous discussion clearly illustrates the effectiveness of the SET protocols in securing electronic transactions using payment cards. The levels of cryptography used by SET are such that only the most powerful adversaries, which basically means governments and other major organisations, would realistically have the resources to break such encryption in any remotely useful timeframe. Of course, as mentioned earlier, key lengths will need to continue to increase commensurately with improvements in cryptanalysis techniques in order for this to remain true. Given that SET is primarily aimed at protecting individual consumers, the possibility of such an organisation dedicating the resources required to the task of acquiring individual payment card information would seem to be remote in the extreme, with possible rare exceptions.

SET uses a sensible balance of conventional and public key cryptography. While it uses the faster conventional cryptography to do the bulk of encrypting, it still uses additional public key cryptography in each message to give added security where needed, and to provide additional authentication, verification and non-repudiation.

The use of certificates, issued from a purpose specific hierarchy of trust, provides a high level of confidence in the authentication process. The special care that is given to maintaining the integrity of the root key guarantees the reliability of this system.

Widespread adoption of the SET protocols could take some time, but not overly so given the care that has been taken to assure that the SET specification incorporates a

high degree of interoperability. Many organisations are already working on, or in some cases already providing, software certified to the current SET standard. A good example of this is CyberCash, which began trials long before SET was conceived of, and now offers SET compliant products as standard.

## 7.1. Payment Systems

From the study provided herein, it would certainly appear that the SET protocols adequately address the primary areas of concern in Electronic Commerce. The only apparent weakness, within the scope of the SET specifications, is the fact that they focus exclusively on payment cards. Current payment cards, Visa's WebCard not withstanding ("WebCard Visa", 1997, [on-line]), by themselves are unlikely to prove adequate to offer a total payment solution to Internet shoppers over the long term due to the advent of Internet micropayments.

Other payment methods such as NetCheque and ecash purport to have small enough transaction fees to meet the need for micropayments. Consequently, in order for the SET protocols to overcome this problem, a number of possible solutions suggest themselves.

First is the introduction of a new form of payment card, possibly by a third party company, which accumulates micropayments until they reach a predetermined amount. The consumer then pays this as a lump sum using a standard payment card type. This would amortise the single transaction fee over a large number of micropayments, thus reducing it to an acceptable amount per transaction.

The second solution is for the SET specifications to be broadened to include a general protocol available to a variety of different payment types. This would have the added advantage of allowing consumers to either consolidate necessary online financial accounts, or at least to be able to easily transfer funds between different accounts.

However, irrespective of the above concerns regarding payment cards, the fact remains; the SET protocols effectively provide a level of security for payment card transactions that should satisfy all but the most hardened cynic.

According to Visa, the future direction of the SET protocols will be primarily towards the integration of new technologies such as smart cards. "Smart" Visa cards will use integrated circuit chips to allow payment cards to store more user information, to provide portable authentication certificates, as well as allowing them to be used as electronic purses ("What's Next?", 1997, [on-line]). This means that users will be able to download cash values from their existing savings accounts and store them on their Visa card for later use. This may offer a solution to the problem of the high transaction charges associated with payment card usage. However, this has yet to be confirmed by the payment card brands.

## 7.2. The Future of Electronic Commerce

In his closing comments on the advantages of commerce on the Internet, Watson (1997) predicts:

> "The late 1990s will see some further debate over the security of the Internet for conducting business. There will be cases of misuse and fraud, [although] probably a reduction over current levels of such activity. The law will have difficulty coping at first and as usual legislation will trail the need, problems of international boundary transaction jurisdiction will arise, governments will figure out how to tax the Internet and by 2005 the vast majority of business world-wide will operate in this environment. Do we expect anything else?"

In the mere eleven months since the above comment was published, much of what was said in it is already proving true. The laws of many nations have indeed been greatly troubled by jurisdictional issues over the past year, and consequent legislation and international agreements have been forged to try to cope with these difficulties. Current legislation in many countries is undergoing constant review in order to facilitate the accelerated growth of Electronic Commerce without compromising national security, as demonstrated by the amendments to the US export policies ("Cryptographic Policies", 1997, [on-line]).

A growing number of businesses are daily exploring the possibilities offered by this new medium, while governments are trying to determine exactly how they can get a larger share of the profits. Financial payment infrastructures are being developed, often with a

helping hand from the major software houses, who are highly motivated by the potential profits of increased software sales and dependency to give the electronic shopping movement greater impetus.

Concerns about the safety of the Internet as a whole are being swiftly addressed, and with the number of users rapidly increasing, it would seem that this is being achieved to the satisfaction of all but the most skeptical.

So, do we expect anything else? The answer has to be "No", given that government, the private sector, and the public all appear to want this brave new world of cyber-shopping. When the resources of the world are focused on making a viable vision become reality, only a brave person would suggest that they will not ultimately succeed. A more pertinent question might then be, "At what cost"?

## 7.3. Future Research

The SET specifications provide protocols that adequately demonstrate all the necessary functionality required for secure Electronic Commerce, including the interoperability to integrate both current and future technologies, and the modularity to adopt new techniques. Considering this, it would seem that the main requirement for future research lies predominantly in the area of payment systems as a whole.

The requirement would appear to exist for the development of a holistic payment system, and the supporting payment infrastructure, which integrates the best attributes of all current payment systems. Retail Electronic Commerce is a new arena of consumerism, with new payment requirements, which requires an equally original

payment system for it to function in an optimal manner. It is probable that the mere adaptation of current payment methods will fall short of providing the most efficient and acceptable solution.

The final solution to this problem will probably incorporate aspects of current payment systems, but with a ubiquitous payment infrastructure that allows users to use all payment methods from a single financial base, and with uniform transaction protocols.

# 8. References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L., Schiller, J. I., & Schneier, B. (1997). The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. [on-line] Available WWW: http://www.crypto.com/key_study/ [July 1997]

A Brief History of Electronic Commerce. [on-line] (1996). Available WWW: http://www.year-x.co.uk/ec/yxwihis.htm [April 1997]

Acquiring Internet Transactions. [on-line] (n.d.). Available WWW: http://www.cybercash.com/cybercash/wp/bankwp.html#introduction [May 1997]

Alexander, M. (1996). The Underground Guide to Computer Security. Massachusetts, USA: Addison-Wesley Publishing Company.

An Introduction to ecash. (1997). [on-line] Available WWW: http://www.digicash.com/index_e.html [September 1997]

Bacard, A. (n.d.). Bacard's Privacy Page. [on-line] Available WWW: http://www.well.com/user/abacard/privacy.html

Bacard, A. (1995). The Computer Privacy Handbook. California, USA: Peachpit Press.

Broiles, G. (1997). Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. [on-line] Available WWW: http://www.jya.com/wa/watoc.htm [October 1997]

Bruce, G., & Dempsey, R. (1997). Security in Distributed Computing. New Jersey, USA: Prentice Hall PTR.

Business Process Redesign. [on-line] (1996). Available WWW: http://www.year-x.co.uk/ec/yxbpr.htm [April 1997]

Changing the Way you do Business. [on-line] (1996). Available WWW: http://www.year-x.co.uk/ec/yxwicha.htm [April 1997]

Cheswick, W. R., & Bellovin, S. M. (1994). Firewalls and Internet Security. Massachusetts, USA: Addison-Wesley Publishing Company.

CommerceNet / Nielsen Internet Demographics Survey. (1997). [on-line] Available WWW: http://www.commerce.net/work/pilot/nielsen_96/#01 [November 1997]

Compliance. (1997). [on-line] Available WWW: http://www.tenthmountain.com/html/compatibility.html [October 1997]

Computer Technology Research Corp. (1996). Security Issues for the Internet and the World Wide Web. South Carolina, USA: Computer Technology Research Corp.

Cryptographic Policies. (1997). [on-line] Available WWW: http://www.epic.org/crypto/ [November 1997]

Current ecash Issuers and Other Licensees. (1997). [on-line] Available WWW: http://www.digicash.com/index_e.html [November 1997]

CyberCash Overview. [on-line] (1997). Available WWW: http://www.cybercash.com/cybercash/info/overview.html [May 1997]

Davies, D. W., & Price, W. L. (1989). Security for Computer Networks. Chichester, England: John Wiley & Sons.

Diffie, W., & Hellman, M. E. (1976: a). New Directions in Cryptography. IEEE Transactions on Information Theory IT-22 (6), 644-654.

Diffie, W., & Hellman, M. E. (1976: b). Multi-User Cryptographic Techniques. AFIPS Conference Proceedings 45 (pp. 109-112).

Digital Signatures. [on-line] (n.d.). Available WWW: http://www.epic.org/crypto/dss/ [September 1997]

Driscoll, M., Jain, G., Lyons, E., Nuckols, J., & Roberts, C. (1997). [on-line] Available WWW: http://mba.vanderbilt.edu/student/mba98/jeffrey.nuckols/secure_online_payment/secure_payments_frames.html [October 1997]

ECA - Aims and Objectives. [on-line] (n.d.). Available WWW: http://www.eca.org.uk/public/aims.htm [April 1997]

Eddings, J. (1994). How the Internet Works. California, USA: Ziff-Davis Press.

EDS, HP and VeriFone Team to Lower Costs and Simplify Operation of Internet Processing Services for Banks and Financial Institutions. (1997, November 5). Business Wire. [on-line] Available WWW: http://www.newspage.com/ [November 1997]

Electronic Commerce. (1997). [on-line] Available WWW: http://www.visa.com/cgi-bin/vee/nt/ecomm/main.html?2+0 [February 1997]

Flexible Working. [on-line] (1996). Available WWW: http://www.year-x.co.uk/ec/yxflex.htm [April 1997]

Ford, W. (1994). Computer Communications Security. New Jersey, USA: PTR Prentice-Hall, Inc.

Ford, W., & Baum, M. S. (1997). Secure Electronic Commerce. New Jersey, USA: PTR Prentice-Hall, Inc.

Freier, A. O., Karlton, P., & Kocher, P. C. (1996). The SSL Protocol Version 3.0. [on-line] Available WWW: http://home.netscape.com/eng/ssl3/ssl-toc.html [October 1997]

Geographics. (1997). [on-line] Available WWW: http://www.cyberatlas.com/geographics.html [October 1997]

Hoffman, D. L., Novak, T. P., & Chatterjee, P. (1995). Commercial Scenarios for the Web: Opportunities and Challenges. [on-line] Available WWW: http://jcmc.huji.ac.il/vol1/issue3/hoffman.html#Barriers to Commercialization [May 1997]

Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1997). Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web. [on-line] Available WWW: http://www2000.ogsm.vanderbilt.edu/papers/anonymity/anonymity2_nov10.htm [October 1997]

Houser, W. (1995). EDI Meets the Internet: General Information. [on-line] Available WWW: http://www.va.gov/publ/standard/edifaq/general.htm#q1 [April 1997]

Just How Strong is RSA in SET? (1997). [on-line] Available WWW: http://www.rsa.com/set/html/howstrong.html [October 1997]

Koops, B-J. (1997). Crypto Law Survey - Overview per country. [on-line] Available WWW: http://cwis.kub.nl/%7Efrw/people/koops/cls2.htm#co [October 1997]

Mankin, E. (1994). The Cheque is in the E-Mail... [on-line] Available WWW: ftp://prospero.isi.edu/pub/netcheque/information/usc-chronicle-941107/netcheque-usc-chronicle-941107.html [October 1997]

Massey, J. L. (1992). Contemporary Cryptology: An Introduction. In Simmons, G. J. (ed.), Contemporary Cryptology. (Pp. 1-39). New York, USA: IEEE Press.

Miller, T. (1997). Interactive Demographics. [on-line] Available WWW: http://etrg.findsvp.com/resfh/anaconf.html [October 1997]

Money on the Internet. [on-line] (n.d.). Available WWW: http://digicash.com/ecash/moneyonnet.html [May 1997]

Morell, J. A., Neal, W., & Fries, V. (1995). Promoting Electronic Data Interchange: Building a Foundation for Support to Small Business. [on-line] Available WWW: http://www.iti.org/eec/edi-surv/edisurv.htm [April 1997]

Netscape Policy on Encryption Export. (1997). [on-line] Available WWW: http://www.netscape.com/newsref/ref/encryption_export.html [October 1997]

Neuman, B. C., & Medvinsky, G. (1995). Requirements for Network Payment: The NetCheque Perspective. [on-line] Available WWW: http://nii.isi.edu/info/netcheque/documentation.html [October 1997]

Neuman, B. C., & Ts'o, T. (1997). Kerberos: An Authentication Service for Computer Networks. [on-line] Available WWW: http://nii.isi.edu/publications/kerberos-neuman-tso.html [October 1997]

Peirce, M. (1997). Payment mechanisms designed for the Internet. [on-line] Available WWW: http://ganges.cs.tcd.ie/mepeirce/Project/oninternet.html [October 1997]

Pfleeger, C. P. (1997). Security in Computing. (2nd ed.). New Jersey, USA: Prentice Hall International.

Pompili, T. (1996). Evolving Internet Security Methods. PC Magazine Online. [on-line] Available WWW: http://www.zdnet.com/pcmag/issues/1508/pcmg0076.htm [October 1997]

Reid, J. (1996). Plugging the Holes in Host-based Authentication. Computers and Security. 15 (8), 661-671.

Schneier, B. (1994). Applied Cryptography. New York, USA: John Wiley & Sons.

Scollay, M. (1997). Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector. [on-line] Available WWW: http://www2.austlii.edu.au/itlaw/national_scheme/national-INFORMAT.html [September 1997]

Secure Electronic Transaction (SET) Specification Book 1: Business Description. (1997). [on-line] Available WWW: http://www.visa.com/cgi-bin/vee/sf/set/downloads.html?2+0 [February 1997]

Secure Sockets Layer. (1997). [on-line] Available WWW: http://home.netscape.com/info/security-doc.html [April 1997]

Sheldon, T. (1997). Windows NT Security Handbook. California, USA: McGraw-Hill, Inc.

Smid, E. S., & Branstad, D. K. (1992). The Data Encryption Standard: Past and Future. In Simmons, G. J. (ed.), Contemporary Cryptology. (Pp. 43-64). New York, USA: IEEE Press.

Some Definitions of Electronic Commerce. (1996). [on-line] Available WWW: http://www.year-x.co.uk/ec/yxwidef.htm [April 1997]

Somlyody, S. (1996). Internet Services Revenue to Hit $30 Billion by the Year 2000. [on-line] Available WWW: http://www.forrester.com/pressrel/AUG96TSP.htm [April 1997]

Stallings, W. (1995). Network and Internetwork Security. Massachusetts, USA: Academic Press, Inc.

Stinson, D. R. (1995). Cryptography: Theory and Practice. Boca Raton, USA: CRC Press, Inc.

The Ease of Using ecash. (1997). [on-line] Available WWW: http://www.digicash.com/index_e.html [September 1997]

The Future. (1996). [on-line] Available WWW: http://www.year-x.co.uk/ec/yxwifut.htm [April 1997]

The Possibilities with Electronic Commerce. [on-line] (n.d.). Available WWW: http://www.cerc.ctc.com/necrc/poss.htm [October 1997]

Till, G. J. (1997). Implications of the Secure Electronic Transactions (SET) Specification on Credit Card Sales over the Internet: For Merchants, the Devil may be in the Details. [on-line] Available WWW: http://www.citynet.net/Personal/till/set1.htm [April 1997]

Visa and MasterCard welcome American Express. (1996). [on-line] Available WWW: http://www.visa.com/cgi-bin/vee/av/news/PR022996.html?2+0 [September 1997]

Watson, A. (1997). Is the Internet a Secure Place for Conducting Business? International Journal of Risk, Security and Crime Prevention, 2 (1), 49-62.

WebCard Visa. (1997). [on-line] Available WWW: http://www.conductor.com/buffer.htm [November 1997]

What are DSA and DSS? (1996). [on-line] Available WWW: http://www.rsa.com/rsalabs/newfaq/q26.html [October 1997]

What's Next? (1997). [on-line] Available WWW: http://www.visa.com/cgi-bin/vee/nt/sec/no_shock/next_L.html?2+0 [November 1997]

White, G. B., Fisch, E. A., & Pooch, U. W. (1996). Computer Systems and Network Security. Boca Raton, USA: CRC Press, Inc.

Why Do We Need Security in Cyberspace? [on-line] (n.d.). Available WWW: http://www.visa.com/cgi-bin/vee/sf/set/setsec.html?2+0 [April 1997]

Wisebrod, D. (1997). The Threat. [on-line] Available WWW: http://www.CataLaw.com/doom/threat.shtml# [November 1997]

# Appendix A

## Payment mechanisms designed for the Internet

| Name | Internet Reference |
|---|---|
| Anonymous Internet Mercantile Protocol | Http://ganges.cs.tcd.ie/mepeirce/Project/Oninternet/aecinet.ps |
| BankNet | Http://mkn.co.uk/bank |
| Brand's Cash | Http://www.cwi.nl/~brands/ |
| BuyWay and BuyWayPS | Http://www.nipactimmedia.com/buyway/introbw.htm |
| CARI | Http://www.netresource.com/ip/cari.html |
| CheckFree | Http://www.checkfree.com/ |
| ClickShare | Http://www.clickshare.com/clickshare/ |
| CommerceNet | Http://www.commerce.net/ |
| Credit Card Network | Http://www.creditnet.com/ |
| Cybank | Http://www.cybank.net/ |
| CyberCash | Http://www.cybercash.com/ |
| CyberSource | Http://www.cybersource.com/ |
| Digital Silk Road | Http://www.agories.com/dsr.html |
| Downtown Anywhere | Http://www.awa.com/ |
| Ecash | Http://www.digicash.com/ |
| Electronic Funds Clearinghouse, Inc. | Http://www.efunds.com/ |
| Electronic Lottery Tickets | Http://theory.lcs.mit.edu/~rivest/lottery.ps |
| Evend | Http://www.evend.com/evend_home.html |
| First Bank of the Internet (defunct) | Http://ganges.cs.tcd.ie/mepeirce/Project/Press/fboi.html |
| First Virtual | Http://www.fv.com/ |
| FSTC Electronic Check Project | Http://www.fstc.org/ |
| Globe ID | Http://globeid.getech.fr/ |
| IKP | Http://www.zurich.ibm.com:80/Technology/Security/extern/ecommerce/iKP.html |
| IPAY | Http://www.ietf.org/ietf-pay/ietf-pay-charter |
| Iwinpak | Http://www.iwinpak.com/ |
| Java Electronic Commerce Framework | Http://java.sun.com/products/commerce/ |
| LETSystems | Http://www.gmlets.u-net.com/ |
| Magic Money | Http://ganges.cs.tcd.ie/mepeirce/Project/Oninternet/mm.html |
| MarketNet | Http://mkn.co.uk:80/ |

| | |
|---|---|
| Micro Payment Transfer Protocol | Http://www.w3.org/TR/WD-mptp |
| Millicent | Http://www.millicent.digital.com/ |
| Mini-Pay | Http://www.ibm.net.il/ibm_il/int-lab/mpay/index.html |
| Mondex | Http://www.mondex.com/ |
| Neosphere Micropayment | Http://www.neosphere.com/ |
| NetBank's NetCash | Http://www.teleport.com/~netcash/ |
| NetBill | Http://www.ini.cmu.edu/netbill/ |
| NetCash | Http://nii-server.isi.edu:80/info/netcash/ |
| NetCheque | Http://nii-server.isi.edu/info/NetCheque/ |
| NetChex | Http://www.netchex.com |
| NetFare | Http://www.netfare.com/ |
| NetMarket | Http://www.netmarket.com/cig/cgi-bin/NetMarket/netMarketMain/ |
| Netscape Communications | Http://home.netscape.com/ |
| Online Bank Listing | Http://www.escapeartist.com/money/money.htm |
| Online Check System | Http://www.onlinecheck.com/ |
| Open Market | Http://www.openmarket.com/ |
| PayMe Transfer Protocol | Http://ganges.cs.tcd.ie/mepeirce/Project/Payme/Overview.html |
| PayWord and MicroMint | Http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps |
| Redi-Check | Http://www.redi-check.com/ |
| Secure-Bank | Http://www.secure-bank.com/ |
| SET | Http://www.visa.com/cgi-bin/vee/st/set/intro.html |
| SecureOrder | Http://www.atsbank.com/demos.htm |
| Security First Network Bank | Http://www.sfnb.com/ |
| SNPP | Http://ganges.cs.tcd.ie/mepeirce/Project/Oninternet/snpp-paper.ps.Z |
| SubScrip | Http://www.cs.newcastle.edu.au/Research/afurche/subscrip.ps |
| Sun Internet Commerce Group | Http://www.sun.com/security/ |
| ZipLock | Http://www.portsoft.com/ |

**(Peirce, 1997, [on-line])**