AUDITING THE VALIDITY OF TRANSACTIONS USING SECURE ELECTRONIC TRANSACTION (SET) PROTOCOLS

by

SUBATHREE PADAYACHY

SHORT DISSERTATION

submitted in partial fulfilment of the requirements for the degree

MASTER OF COMMERCE

in

COMPUTER AUDITING

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

at the

RAND AFRIKAANS UNIVERISTY

STUDY LEADER: PROF A DU TOIT

JOHANNESBURG
NOVEMBER 1997

ACKNOWLEDGEMENTS

The opinions expressed and the conclusions made, are those of the author, and should not be seen as the opinions and conclusions of anyone else.

A word of special appreciation to the following:

- Prof du Toit and Prof Boshoff, for their continual assistance and support during the two years of study.
- My family and friends, for their unconditional support and understanding. I am proud to dedicate this document to my parents and late grandmother for all their love, patience, encouragement and years of sacrifice.
- To God, all the glory.

OPSOMMING

OUDITERING VAN DIE GELDIGHEID VAN TRANSAKSIES DEUR GEBRUIK VAN SET PROTOKOLS

DEUR

SUBATHREE PADAYACHY

OPSOMMING VAN DIE SKRIPSIE ONGEDIEN VIR DIE GRAAD MAGISTER COMMERCII IN REKENAAROUDITERING
IN DIE FAKULTEIT EKONOMIESE EN BESTUURWETENSKAPPE
AAN DIE RANDSE AFRIKAANSE UNIVERSITEIT

STUDIELEIER: PROF A DU TOIT

JOHANNESBURG
NOVEMBER 1997

INDEX

Die doel met die opsomming is om die agtergrond, metodiek en gevolgtrekkings van die navorsing oor die ouditering van geldigheid van transaksies deur die gebruik van SET protokols te bespreek. Hierdie opsomming is onder die volgende hoofde uiteengesit:

1. PROBLEEMBESKRYWING EN DOEL MET HIERDIE KORT SKRIPSIE
2. NAVORSINGS METODOLOGIE
3. OMVANG EN BEPERKINGS
4. RESULTATE
5. GEVOLGTREKKING

1. PROBLEEMBESKRYWING EN DOEL MET HIERDIE KORT SKRIPSIE

'n Beraamde 60 miljoen mense maak gebruik van die Internet en 'n groei van 10% per maand word voorspel. Die geweldige uitbreiding van die Internet word grootliks aangevuur deur die vooruitsig om besigheid aanlyn te doen. Die oorspronklike Internet was ontwerp vir navorsing en nie vir kommersiële transaksies nie, en daar is staatgemaak op die integriteit van die gebruikers. Die TCP/IP protokol skep verskeie inherente swakhede rakende sekuriteit. Derhalwe is die ontwikkeling van SET as 'n oop, nie-kompeterende, vry, en tussen-werkende standaard verwelkom deur kommersiele en finansiële industrie.

Die bekommernis is dat SET nie die volgende funksionaliteite dek nie nl. vertroulikheid, bemagtiging, integriteit van data, nie-verwerping, en toegang tot dienste.

Die doel van hierdie skripsie is om 'n oudit program te ontwikkel wat die geldigheid van transakasies deur die gebruik van die SET protokol aan sal spreek.

2. NAVORSINGS METODOLOGIE

- 'n Literatuur oorsig is gedoen deur die gebruik van bestaande gesaghebbende artikels, publikasies, boeke en ander literatuur soos bv. die Internet. Hierdie oorsig is gedoen op veilige kommersiële transaksies en die vereistes en implementering van SET.

- 'n Gestruktureerde vraelys is ontwikkel en onderhoude gereël om terugvoer te verkry op addisionele gëidentifiseerde kontrole swakhede.
- Met al die inligting wat verkry is uit die literatuur oorsig, is 'n oudit program ontwikkel vir die toetsing van die geldigheid van transaksies deur die gebruikmaking van SET protokol transaksies.

3. OMVANG EN BEPERKINGS

Hierdie kort skripsie fokus op die SET proses en bepaal of dit transaksies effektief kontroleer vir geldigheid. Vir die doel van hierdie kort skripsie word slegs die volgende in die omvang ingesluit :

- Toepassing van kriptografiese algoritmes (byvoorbeeld DES en RSA);
- Sertifikaat boodskappe en doelformate;
- Aankoops boodskappe en doelformate;
- Magtigings boodskappe en doelformate; en
- Boodskap protokols tussen partye.

Sekere uitsluitings is spesifiek van toepassing op hierdie kort skripsie :

- Boodskapprotokols vir aanbiedings, inkopies, goedere aflewering, ens.;
- Operasionale kwessies soos die kriteria bepaal deur finansiële instellings vir die uitreiking van kaarthouer en handelaar sertifikate;
- Skerm-formaat insluitende die inhoud, aanbieding, en uitleg van bestelling intree forms, soos gedefinieer deur die handelaar;
- Algemene betalings bo en behalwe die area van betalingskaarte; en
- Sekuriteit van kaarthouer, handelaar, en betalings toegangshek ("gateway") stelsel data insluitende beskerming teen virusse, Trojaanse perd programme, en inbrekers ("hackers").

4. UITSLAE

Die uitslag van hierdie studie is 'n detail oudit-program wat die geldigheid van transaksies deur die gebruik van SET protokols aanspreek.

SET is 'n oop, vry, nie-kompeterende, en tussenwerkende standaard wat deelnemers toelaat om op 'n veilige wyse, aanlyn te handel. Die risiko's van vertroulikheid, bemagtiging, integriteit van data, nie-verwerping, en toegang tot dienste is sleutel vereistes vir 'n veilige kommersiële transaksie. Vir die doel van hierdie studie is 'n kontrole raamwerk ontwikkel om die doeltreffendheid van kontroles vir kommersiële transaksies te bepaal.

5. GEVOLGTREKKING

Die hoof probleem wat geïdentifiseer is, is die tekort aan sekuriteit in die TCP/IP protokol stel. Dit het die vereiste aan die ontwikkeling van 'n produk soos SET genoodsaak. Dit was egter nodig om te evalueer of SET die sleutel bekommernisse wat in 'n kommersiële transaksie identifiseer is, aanspreek. Hierdie belangrikste bekommernisse is vertroulikheid, bemagtiging, integriteit van data, nie-verwerping, en toegang tot dienste.

Ter opsomming, hierdie navorsing verskaf die basis om die SET proses, sleutel komponente, en hul vereistes te verstaan, sowel as die vraag na hoe die risikos wat geïdentifiseer is, aangespreek kan word.

Die oudit-program wat ontwikkel is, is nie bedoel om goeie Internet sekuriteitsbestuur en onderhoud te vervang nie, maar dit kan die ouditeur ondersteun om die waarde wat verskaf word, te optimaliseer.

SYNOPSIS

1. PROBLEM DESCRIPTION AND OBJECTIVE OF THIS SHORT DISSERTATION

There is an estimated 60 million people using the Internet with an estimated growth of 10% per month. The Internet explosion has been largely fueled by the prospect of conducting business online. The original Internet was designed for research, and not for commercial transactions and the integrity of the users was relied upon . The TCP/IP protocol suite has many inherent security weaknesses. Therefore the development of SET as an open, non-competitive, free and interoperable standard was welcomed by the commercial and financial industries.

The concern is that SET does not perform the following functionalities in terms of confidentiality, authentication, integrity of data, nonrepudiation and access to services.

The objective of this short dissertation is therefore to develop an audit program to audit the validity of transactions using SET protocols.

2. RESEARCH METHODOLOGY

- A literature survey has been done on existing authoritative articles, publications, books and other literature, such as the Internet, on secure commercial transactions and the requirements and implementation of SET.
- A structured questionnaire was developed and interviews arranged to obtain feedback on additional control weaknesses identified.
- With all the information obtained in the literature survey, an audit program for the validity of transactions using SET protocols has been developed.

3. SCOPE AND LIMITATIONS

This short dissertation focuses on the SET process and whether it effectively validates transactions. For the purpose of this short dissertation only the following are within the scope :

- Application of cryptographic algorithms (such as DES and RSA);
- Certificate message and object formats;
- Purchase messages and object formats;
- Authorisation messages and object formats;
- Capture messages and object formats; and
- Message protocols between parties.

Certain exclusions specifically apply to this short dissertation:

- Message protocols for offers, shopping, delivery of goods, etc.;
- Operational issues such as the criteria set by individual financial institutions for the issuing 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; and
- Security of data on cardholder, merchant, and payment gateway systems including protection from viruses, Trojan horse programmes, and hackers.

4. RESULTS

A detailed audit program to audit the validity of transactions using SET protocols has been developed as a result of this study.

SET is an open, free, non-competitive and interoperable standard that allows participants to transact online in a secure manner. The risks of confidentiality, authentication,

integrity of data, nonrepudiation and access to services are key requirements in a secure commercial transaction.

For the purpose of this study, a control framework to assess the adequacy of controls for commercial transactions has been developed.

5. CONCLUSION

The main problem identified is the lack of security within the TCP/IP protocol suite, which necessitated the development of a product like SET. However, we needed to evaluate whether SET addressed the key concerns that were identified in a commercial transaction viz. Confidentiality, authentication, data integrity, nonrepudiation and access to services.

Further academic research on SET and secure commercial transactions has to be performed once financial institutions have fully implemented the open standard. Additional risks may be identified with changes in hardware and software architectural developments.

In summary, this research has provided the basis for understanding the SET process, key components, requirements and how the risks identified can be addressed.

The audit program which has been developed is not meant to be a replacement for good Internet security management and maintenance, but it can assist the auditor in optimising the value being provided.

CHAPTER 1 - INTRODUCTION

This study is intended to develop a scientific model / audit programme for auditing the validity of transactions using SET protocols. The objective of this chapter is to provide background information about research in the area of Secure Electronic Transaction protocols. This chapter is presented under the following headings:

1.1 BACKGROUND

1.2 PROBLEM DESCRIPTION

1.3 OBJECTIVE OF THIS RESEARCH

1.4 DEFINITIONS

1.5 SCOPE, LIMITATIONS AND EXCLUSIONS

1.6 RESEARCH METHODOLOGY

1.7 RESEARCH APPROACH

1.8 SUMMARY OF RESULTS

1.9 CONCLUSIONS

1.1 BACKGROUND

1.1.1 Growth Of The Internet

SET stands for Secure Electronic Transactions and is a proposed standard for performing credit card transactions over the Internet. It is being developed jointly by Visa and MasterCard, with technical assistance from various Internet, Information systems, and cytology companies such as Netscape, IBM and VeriSign. With these names behind it, SET may very well become the dominant method for paying by credit card over the Internet. MasterCard and Visa are developing SET as a license-free protocol for credit card transactions over the Internet.

In total there are currently more than seven million computers connected to the Internet, with an estimated 60 million people using Internet resources. The Internet's estimated growth rate is to be growing at a rate of ten percent per month. Since the Internet is growing so rapidly, at any given moment more than half of the user community has been on the Internet for less than one year. New users are thus more common than experienced users. A survey conducted in South Africa in January 1996, found 48 277 connected computers with an estimated 241 000 Internet users. This placed South Africa eighteenth in the world in terms of Internet connectivity (Quelch & Klein, 1996:7).

The rapid growth of the Internet has a number of effects. Metcalfs Law states that:

"The value of a network - defined as its utility to a population - is roughly proportional to the number of users squared.

This implies that the larger the Internet becomes, the more it will be used. The commercial domain is the largest and fastest growing domain on the Internet. Eighty percent of new network registrations are for commercial concerns (Tibaldeo & Buben,

1996:19). This indicates the important role that the Internet will play in business in the future.

1.1.2 Goals of SET

There are several goals to be achieved by creating this protocol.

1. The creation of a simple inexpensive way for merchants to conduct credit card sales over the Internet;
2. The production of a protocol for processing credit card transactions that would have little impact on the existing financial infrastructure;
3. The SET protocol will allow software vendors to produce credit card payment software that will inter-operate; and
4. SET will create a level playing field and ensure competition among software vendors. This will keep costs down for merchants and financial institutions interested in processing credit card payments over the Internet (Tibaldeo & Buben, 1996:19).

There are similarities between CyberCash payment system and SET protocols i.e. the merchants and the buyers will both need software which follows SET protocol in order to use SET for credit card transactions. Acquiring banks process credit card transaction requests delivered to them through SET in much the same way as the process requests originating from a point of sale terminal. Merchants can request the same type of transactions (authorise, authorise and capture, etc.) as they can through CyberCash (Anon., 1997b:10).

1.1.3 Differences Between SET And Cybercash

Some of the major differences between the two payment systems are as follows:

- CyberCash takes an active role in processing each credit card transaction that flows through the system;
- With SET, there is no single company which will be responsible for processing the transactions;

- Cybercash's server sits between the merchant and the acquiring bank;
- The task of translating from SET request format to the format used by acquiring banks is done by the SET payment gateway. These gateways can either be run by companies contracted by the acquiring banks to do so on their behalf, or by the acquiring banks themselves;
- SET verifies the identity of the buyer and the merchant involved in the transaction; and
- Identity verification of buyers, merchants, and acquiring banks is not handled by a centralised server. SET uses a system of certificates for party verification. Certificates are like the stamp a notary public places on a document to confirm the signatures on it. The certificate shows that the signature has been proven to belong to the party in question. The certificates are passed between the buyer's, merchant's, and acquirer's payment gateway software to prove that each entity involved in the transaction is who they claim to be (Anon., 1997b:10).

1.1.4 Electronic Shopping Experience

The following example in Table 1.1 outlines a scenario involving a merchant requesting authorisation of the credit card transaction at the time of sale, and then requesting the actual capture at a later time:

The electronic shopping experience can be divided into several distinct stages: Although these stages are listed in a specific order, variations on this order are possible (Anon., 1997b:10).

Stage	Description
1	The cardholder browses for items in a variety of ways, such as: *using a browser to view an online catalogue on the merchant's World Wide Web page; * viewing a catalogue supplied by the merchant on a CD-ROM; or * looking at a paper catalogue.
2	The cardholder selects items to be purchased.
3	The cardholder is presented with an order form containing the list of items, their prices, and a total price including shipping, handling, and taxes. This order form may be delivered electronically from the merchant's server or created on the cardholder's computer by electronic shopping software. Some online merchants may also support the cardholder's ability to negotiate the price of items (such as by presenting frequent shopper identification or information about a competitor's pricing).
4	The cardholder selects the means of payment. This specification focuses on the case where a payment card is selected.
5	The cardholder sends the merchant a completed order along with payment instructions. In these specifications, the order and the payment instructions are digitally signed by cardholders who possess certificates.
6	The merchant requests payment authorisation from the cardholder's financial institution.
7	The merchant sends confirmation of the order.
8	The merchant ships the goods or performs the requested services from the order.
9	The merchant requests payment from the cardholder's financial institution.

TABLE 1.1 ELECTRONIC SHOPPING EXPERIENCE (Anon., 1997b:10)

1.1.5 Advantages And Disadvantages of SET

The SET protocol provides the following advantages and disadvantages over other payment systems:

ADVANTAGES:

- Eliminates the need for a third party to monitor Internet credit card transactions. This will lower the cost of doing credit card business over the Internet;
- Strong encryption and authentication scheme to be used;
- Merchant does not have access to the buyer's credit card number;
- Merchants do not have a waiting period for receiving payment, as with First Virtual. The merchant's bank account gets credited within the usual time frame for credit card transactions; and
- Is backed by VISA and MasterCard.

DISADVANTAGES:

- It is not yet ready for use . The SET protocol was only released for public comment in February 1996;
- Buyers and merchants will need to install software which allows for SET transactions processing. Acquiring banks will either need to contract with a company to run a SET Internet gateway for them, or install a SET Internet gateway themselves; and
- Merchants will need to have an account with an acquiring bank or card processor that is set up to accept SET transactions (Anon., 1997b:12).

1.2 PROBLEM DESCRIPTION

There is still disagreement as to whether or not the Internet is an appropriate tool for conducting business transactions. Due to the distributed nature of the Internet, temporary

or total communication failures are inevitable. This leads to situations where a reputable merchant may be unable to deliver merchandise which has been paid for, or even notify the buyer of its non-delivery. Since the Internet was designed for research, security was an afterthought in design. Security relied on users mutual respect and knowledge of appropriate action (Bhimani, 1996:29). In addition, most Internet users are still in the browsing mode of Internet exploration and have not used the Internet to buy goods (Payne & Pool, 1995:27). Despite these limitations a number of authors believe that the Internet will be used to conduct business.

By the year 2008, twenty percent of all groceries will be bought electronically. Others are less optimistic, believing that only a limited number of products will be traded on the Internet (Payne & Pool 1995:27). The products that can be traded must fit the demographic profile of Internet users, be easily presented in electronic form using limited bandwidth and must not be controlled by trade regulations. Currently 64% of purchases on the Internet are for computer software and hardware, books, music and magazines. This implies that products with low prices sell better (Quelch & Klein, 1996:7). Regardless of the products that are traded, the Internet will have a profound effect on industry structure.

With more than 30 million Internet users today, and 90 million projected to come on board in the next two years, the Internet is a new way for businesses to establish computer-based resources that can be accessed by consumers as well as business partners around the world (Anon., 1997d:1).

1.3 OBJECTIVE OF THIS RESEARCH

The objective of this short dissertation is to develop an audit program for auditing the validity of credit card transactions over the Internet using the SET protocols.

1.4 DEFINITIONS

SET (Secure Electronic Transaction) is defined as the set of open standards jointly developed by Mastercard and Visa with technical assistance from various Internet and Information systems including IBM, and Netscape. It is a technical specification for securing payment card transactions over open networks such as the Internet (Anon., 1997b:12).

A transaction for this discussion is limited in definition to cover the completed order information and payment instruction, the payment authorisation request, confirmation of order and request for payment.

1.5 SCOPE, LIMITATIONS AND EXCLUSIONS

SET is a payment protocol designed to protect consumer's bankcard information when they choose to use bankcards to pay for goods and services on the Internet and other open networks. SET does not go beyond that scope or explores areas that are being addressed by the computer industry; specifically, it does not define the shopping or ordering process; it does not define payment method selection (such as credit card, check or mail order), and it does not address platform, device or operating system security.

Although hardware and software such as firewalls, routers and proxy servers are critical in the security of Internet connectivity, these issues all fall outside of the scope of this dissertation.

1.6 RESEARCH METHODOLOGY

The following methodolgy has been used:

- A literature survey has been performed of authoritative articles, publications and books relating to :
  commercial transactions on the Internet;
  Internet security issues; and
  requirements and implementation of SET.
- Structured interviews with experts on SET were conducted.

- With all the information obtained in the literature survey, an audit program was compiled to audit the validity of transactions using SET protocols.

1.7 RESEARCH APPROACH

In this chapter the need for a standard like SET and the subsequent auditing thereof, was established. The need for an audit program addressing the validity of transactions using SET protocols for the auditor to rely on the validity of data, has been established.

In Chapter 2, the problems and risks of commercial transactions over the Internet are discussed, as well as how SET has the necessary controls to overcome these loopholes. Confidentiality, authentication, integrity of data and nonrepudiation have all been addressed to satisfy audit requirements.

In Chapter 3, a structured questionnaire was developed as a control framework to assess the adequacy of controls, and interviews were set up to obtain input about additional risks and concerns. An audit program to audit the validity of transactions using the SET protocols is developed in Chapter 4. Finally, Chapter 5 concludes the short dissertation and indicates whether the objective of the short dissertation has been met. Figure 1.1 depicts the structure of the rest of this short dissertation.

CHAPTER 1

INTRODUCTION

CHAPTER 2

LITERATURE SURVEY

CHAPTER 3

EMPIRICAL STUDY

CHAPTER 4

COMPILATION OF AN AUDIT PROGRAM

CHAPTER 5

CONCLUSION

FIGURE 1.1 STRUCTURE OF SHORT DISSERTATION

1.8 SUMMARY OF RESULTS

There is an estimated 60 million people using the Internet with an estimated growth of 10% per month. The Internet explosion has been largely fueled by the prospect of conducting business online. However, many significant risks were identified which needed to be addressed.

SET provided a standard which addressed the issues of confidentiality, authentication, data integrity, nonrepudiation and access to services.

An audit program has been compiled to audit the validity of transactions using SET protocolsto determine if it could ensure the integrity of information. The implementation of SET to secure commercial transactions needs to be complemented by additional measures including adequate Internet connectivity procedures, physical and logical security, anti-virus screens and Internet security policies, procedures and standards.

1.9 CONCLUSIONS

A detailed audit program to validate transactions using SET protocols has been developed.

This audit program can be utilised by the auditor, to determine if the implementation of SET will effectively ensure the validation of transactions.

This audit program could also be used to provide an additional client service for the evaluation of the adequacy of a client's Internet security strategy.

This audit program should be used in addition to the detailed computer auditing programs.

The implementation of SET addresses the risks of confidentiality, authentication, data integrity, nonrepudiation and access to services. However, the implementation of SET alone will ensure not the validity of commerical transactions. It should therefore be used in conjunction with other security mechanisms to limit Internet security risks. It therefore opens new fields for academic research in the evaluation of the remaining security mechanisms.

CHAPTER 2 - LITERATURE SURVEY

This chapter is presented under the following headings:

2.1 OBJECTIVE

2.2 NATURE OF LITERATURE SURVEY

2.3 SCOPE, LIMITATIONS AND EXCLUSIONS

2.4 DEFINITIONS

2.5 BACKGROUND

2.6 SECURITY REQUIREMENTS FOR COMMERCIAL TRANSACTIONS

2.7 CONCLUSION

2.1 OBJECTIVE OF THE LITERATURE SURVEY

The objective of the literature survey is to provide a generic audit programme for auditing the validity of transactions using SET protocols. This chapter provides definitions and information on the key elements intrinsic in a credit card transaction, some of the problems inherent in the TCP/IP suite, security requirements as well as security initiatives being taken.

2.2 NATURE OF THE LITERATURE SURVEY

To ensure credibility and acceptance of the findings and proposal of this short dissertation, it is essential that the underlying concepts be based on authoritative views and be generally accepted among auditing professionals. Theory based on an individual's experience without taking generally accepted professional views into account, may be subject to personal bias. Other factors which may introduce bias are the individual's background and the absence of formal research. To avoid these problems, references have been restricted to authoritative technical books, articles and publications by computer experts. The main categories of authors/publishers are:

- Experts i.r.o. SET; and
- Mastercard.

The reasons for choosing these authors / publishers are as follows:

- They represent, between them most of the internationally accepted views on SET;
- The emphasis on auditor-related references provide a wider background for finding risks relevant to the auditor involved in SET; and
- As a group, they represent a properly balanced view of SET.

2.3 SCOPE, LIMITATIONS AND EXCLUSIONS

The SET specification addresses a portion of the message protocols that are necessary for electronic commerce. It specifically addresses those parts of the protocols that use or impact the use of payment cards.

Based on the electronic shopping experience set out in Chapter 1, stages 5, 6, 7, and 9 will be within the scope of this project. The following are within the scope of this specification:

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

The following are outside of the scope of this research:

- Message protocols for offers, shopping, delivery of goods, etc.;
- Operational issues such as the criteria set by individual financial institutions for the issuing 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; and
- Security of data on cardholder, merchant, and payment gateway systems including protection from viruses, Trojan horse programmes, and hackers.

The above have been specifically excluded since they do not directly impact the validity of transactions. The focus is on the stage that the cardholder chooses to use a payment card as the means of payment, thereby excluding the above stages.

2.4 DEFINITIONS

SET changes the way that participants in a payment system interact. In a face-to-face retail transaction or a mail order transaction, electronic processing begins with the merchant or the acquirer. However, in a SET transaction, the electronic processing begins with the cardholder, as described in Figure 2.1.

- **Cardholder**

  In the electronic commerce environment, consumers and corporate purchasers interact with merchants by means of personal computers. A cardholder uses a payment card that has been issued by an Issuer. SET ensures that in the cardholder's interactions with the merchant, the payment card account information remains confidential (Anon., 1997b:12).

- **Issuer**

  An issuer is a financial institution that establishes an account for the cardholder and issues the payment card. The issuer guarantees payment for authorised transactions using the payment card in accordance with payment card brand regulations and local legislation (Anon., 1997b:12).

- **Merchant**

  A merchant offers goods for sale or provides services in exchange for payment. With SET, the merchant can offer its cardholders secure electronic interactions. A merchant that accepts payment cards must have a relationship with an acquirer(Anon., 1997b:12).

- **Acquirer**

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

- **Payment Gateway**

  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(Anon., 1997b:12).

- **Brand**

  Financial institutions have founded payment card brands that protect and advertise the brand, establish and enforce rules for use and acceptance of their payment cards, and provide networks to interconnect the financial institutions. Other brands are owned by financial services companies that advertise the brand, and establish and enforce rules for use and acceptance of their payment cards. These brands combine the roles of issuer and acquirer in interactions with cardholders and merchants.

- **Third parties**

  Issuers and acquirers sometimes choose to assign the processing of payment card transactions to third-party processors. This document does not distinguish between the financial institution and the processor of the transactions (Anon., 1997b:13).

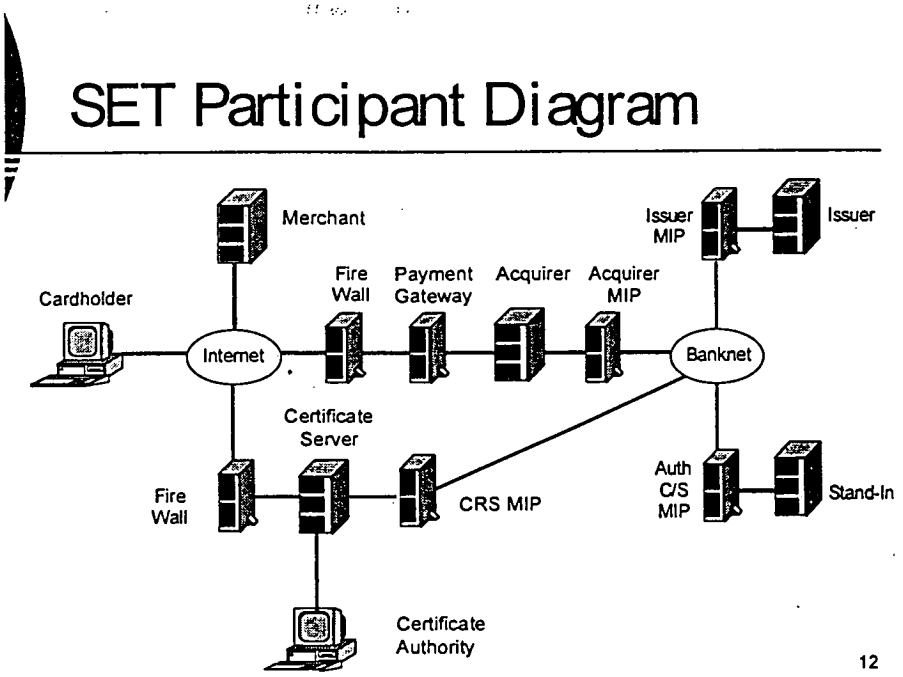

FIGURE 2.1 SET PARTICIPANTS (Anon., 1997b:12)

2.5 BACKGROUND

The SET payment process is slightly more complicated than the others discussed because of the need to pass public keys between parties and verify certificates during the transaction. The current trend of payment methods for online transactions is as follows:

Credit Card : 87%
Cheque in Mail : 10%
Cheque on delivery : 5%
Cash on delivery : 1%
Digital cash : 0% (Anon., 1997d:3).

The Internet is changing the way we access and purchase information, communicate and pay for services, and acquire and pay for goods. Financial services such as bill payment, brokerage, insurance, and home banking are now or soon will be available over the Net. Any organisation can become a global publisher by establishing an information site on the Internet's World Wide Web (Anon., 1997c:1).

There is no question that electronic commerce is going to have an enormous impact on the financial services industry, as exemplified by the popularity of the Internet. No financial institution will be left unaffected by the explosion of electronic commerce.

- The number of payment card purchases made through this medium will grow as Internet-based online ordering systems are created;
- Many banks are planning to support this new form of electronic commerce by offering card authorisations directly over the Internet; and
- Several trials with electronic currency and digital cash are already under way (Mastercard and Visa select Terisa, 1996:1).

The original Internet was designed for research, and not as a commercial environment. As such, it operated in a single domain of trust. While provisions were made to allow remote users to access critical files on machines, Security generally relied on the users' mutual respect and honour as well as their knowledge of conduct, which was considered appropriate on the network. Minor security (password-protection) was provided as an afterthought. As the Internet has grown, we have seen evidence of Internet-based attacks on commercial systems. Normally, attackers take advantage of simple holes due to misconfigured systems, poorly written software, mismanaged systems, or user neglect. Network security tools, such as firewalls are being used to protect individual networks from attack. More sophisticated attacks can take advantage of the basic flaws in the Internet's infrastructure. For example, the TCP/IP protocol suite used by all computers connected to the Internet is fundamentally lacking in security services (Bhimani, 1996:29).

The most glaring omissions occur at the lower layers of the protocol stack - within TCP, IP, and such transmission protocols as Ethernet. Since they affect all applications that rely on the transport mechanism, an attack can take a number of forms:

- Eavesdropping on a network results in theft of account information, such as credit card numbers, customer account numbers, or account balances and billing information, and theft of services normally limited to subscribers. This also constitutes an invasion of one's privacy; etc.
- Password "sniffing" attacks are used to gain access to systems containing proprietary information. The use of stronger cryptographic algorithms will see a shift away from attempts to break the protocol toward retrieving cleartext information from poorly protected systems; etc.
- Data modification attacks can be used to modify the contents of certain transactions (e.g. changing the payee on an electronic cheque or changing the amount being transferred to a bank account);
- "Spoofing" attacks are used to enable one party to masquerade as another party. A criminal can set up a storefront and collect thousands or even millions of credit card numbers, account numbers, or other information from unsuspecting consumers. An
- individual could pose as a financial clearing-house or acquirer, and collect payment from unsuspecting consumers or fees from merchants; and
- Repudiation of transactions can cause major problems with billing systems and transaction-processing agreements. If one party reneges on an agreement after the fact, the other party may incur the cost of transaction processing without benefiting from the transaction (Bhimani, 1996:30).

SET addresses seven major business requirements which can adequately cover the risks identified:

1. Providing confidentiality of payment information and enabling confidentiality of order information that is transmitted along with the payment information.
2. Ensuring the integrity of all transmitted.
3. Provision of authentication that a cardholder is a legitimate user of a branded payment card account.
4. Provision of authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
5. Ensuring the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
6. Creation of protocol that neither depends on transport security mechanisms nor prevents their use.
7. Facilitation and encouragement of interoperability among software and network providers (Anon., 1997d:6).

2.6 SECURITY REQUIREMENTS FOR COMMERCIAL TRANSACTIONS

This sub-section will be further examined under the following headings:

2.6.1 LACK OF SECURITY SERVICES IN THE TCP/IP PROTOCOL SUITE

2.6.2 A ROBUST SECURITY SYSTEM

2.6.3 SECURITY INITIATIVES

2.6.4 CRYPTOGRAPHY

2.6.5 DUAL SIGNATURES

2.6.6 CERTIFICATE ISSUANCE

2.6.1 Lack Of Security Services In The Tcp/Ip Protocol Suite

While firewalls serve a valuable purpose in securing Internet-connected networks, they do not provide end-to-end transaction security and cannot be considered adequate security solutions for commercial Internet transactions (Bhimani, 1996:30).

There is a fundamental lack of security services in the TCP/IP protocol suite:

- **Lower-layer protocols**

Most lower-layer protocols, including Ethernet, are "broadcast" in nature. It is possible for any machine connected to a local area network (LAN) to "eavesdrop" on traffic destined for other machines on the same LAN. Any machine on the Internet that happens to lie along a path between two communicating parties (e.g. a service provider) can "eavesdrop";

- **Authentication**

No protocol in the entire TCP/IP suite contains any authentication of the communicating parties. It is virtually impossible to accurately determine whether the addresses in data packets are genuine or not, thereby encouraging "impersonation";

- **Packet contents**

There are no measures to authenticate the contents of packets. Although simple checksums are used for error detections in some protocols, these are easily circumvented, thereby leading to data modification; and

- **Sequence numbers**

Certain implementations of TCP make use of easily guessed sequence numbers. The ability to predict TCP sequence numbers coupled with the lack of authentication in TCP, makes it possible to establish fraudulent connections to unsuspecting systems without raising any alarms on legitimate systems (Bhimani, 1996:30).

With open networks, payments will increasingly be made by consumer-driven devices. As advanced technologies become more practical and affordable, the marketplace will move from "brick and mortar" to more convenient locations such as the home or office. As financial services evolve, consumers will consolidate their payment needs into one, multi-functional relationship product that enables widespread, around-the-clock access.

Due to the anonymous nature of communications networks, existing procedures used in face-to-face or mail order \ telephone order (MOTO) transactions including the authentication of the cardholder by the merchant, must be replaced by new procedures. There is also a need for the cardholder to authenticate the fact that the merchant accepts SET transactions and is authorised to accept payment cards (Anon., 1997d:2).

2.6.2 A robust security system

A robust security solution for transaction processing satisfies the following security requirements:

Confidentiality All communication between parties is restricted to the parties involved in the transaction. This confidentiality is an essential component in user privacy, as well as in the protection of proprietary information and as a deterrent to theft of information services (Anon., 1996c:31).

Authentication	Both parties should be able to feel comfortable that they are communicating with the party with whom they think they are doing business. Authentication is usually provided through digital signatures and certificates.
Data integrity	Data sent as part of a transaction should not be modifiable in transit. Similarly, it should not be possible to modify data while in storage.
Nonrepudiation	Neither party should be able to deny having participated in a transaction after the fact.
Selective application of services	It may be desirable for part of a transaction to be hidden from view while the remainder of the same transaction is not(Anon., 1996c:31).

Confidentiality is usually provided through encryption. Authentication, data integrity, and nonrepudiation are usually provided through dual signatures and public-key certificates. These first four requirements are fairly standard for business communications. The fifth, however, raises an important issue. Consider the following case; a customer wants to buy something from a given merchant. Under the standard model, the customer hands his or her credit card to the merchant, who sends the number to the financial institution to be processed. However, this model unnecessarily gives the merchant access to the customer's credit card number (Bhimani, 1996:31).

2.6.3 Security Initiatives

In order to provide these services, a number of cryptographic protocols have been proposed. While these protocols are similar in the service they provide and in the cryptographic algorithms they use, they vary in the manner in which they provide the services and in their locations, with respect to the rest of the TCP/IP protocol stack. Some initiatives endeavour to implement security at the network IP layer; just above TCP, at the session layer; still others, such as ftp., HTTP, and telnet, within specific application protocols, and a whole class of solutions for securing the content of documents residing above the existing application protocols.

The issue of where within the protocol stack to provide security is a contentious one. Proponents of placing security lower in the stack argue that lower-layer security solutions can be implemented transparently to end users and application developers, effectively killing many birds with a single stone. Proponents of higher-layer solutions argue that lower-lay solutions attempt to do too many things and that application-layer solutions allow application-specific security services (Bhimani, 1996:31).

Security issues regarding electronic commerce must be viewed as non-competitive in the interests of financial institutions, merchants, and cardholders.

These requirements are addressed by the following features :

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication
- Interoperability

However, these components do not function independently; all security functions must be implemented (Anon., 1996d:7).

2.6.1.2 Confidentiality of information

To facilitate and encourage electronic commerce using payment card products, it will be necessary to assure cardholders that their payment information is safe and can only be accessed by the intended recipient. Therefore, cardholder account and payment information must be secured as it travels across the network, preventing interception of account numbers and expiration dates by unauthorised individuals. In today's on-line shopping environment, payment instructions containing account information are often transmitted from cardholders to merchants oven open networks with few security precautions, if any. However, this account information provides the key elements needed to create counterfeit cards and/or fraudulent transactions.

While it is possible to obtain account information in other environments, there is a heightened concern about the ease of doing so with public network transactions. This concern reflects the potential for high-volume fraud, automated fraud (such as using filters on all messages passing over a network to extract all payment card account numbers from a data stream), and the potential for "mischievous fraud" that appears to be characteristic of some hackers. In addition, the transmission of account information in a relatively unsecured manner has triggered a great deal of negative press (Anon., 1997d:7).

2.6.1.3 Integrity of data

The specification must guarantee that the message content is not altered during the transmission between the originator and the recipient. Payment information sent from cardholders to merchants includes order information, personal data, and payment instructions. If any component is altered in transit, the transaction will not be processed accurately. To eliminate this potential source of fraud and / or error, SET must provide the means to ensure that the contents of each order and payment message received match the contents of the message sent. SET provides for digital signatures, which ensure the integrity of payment information(Anon., 1997d:7).

2.6.1.4 Cardholder account authentication

Merchants need a way to verify that a cardholder is a legitimate user of a valid, branded payment card account number. A mechanism that uses technology to link a cardholder to a specific payment card account number will reduce the incidence of fraud and therefore the overall cost of payment processing. SET uses digital signatures and cardholder certificates to ensure the authentication of the cardholder account.

2.6.1.5 Merchant authentication

The specification must provide a way for cardholders to confirm that a merchant has a relationship with a financial institution allowing it to accept payment cards. Cardholders also need to be able to identify merchants with whom they can securely conduct electronic commerce. SET provides for the use of digital signatures and cardholder certificates to ensure the authentication of the merchant(Anon., 1997d:7).

2.5.1.6 Interoperability

The specification must be applicable on a variety of hardware and software platforms, and must not include a preference for one over another. Any cardholder with compliant software must be able to communicate with any merchant software that also meets the defined standard. SET interoperability uses specific protocols and message formats to provide interoperability.

2.6.2 CRYPTOGRAPHY

Cryptography has been used for centuries to protect sensitive information as it is transmitted from one location to another. In a cryptographic system, a message is encrypted using a key. The resulting ciphertext is then transmitted to the recipient where it is decrypted using a key to produce the original message. There are two primary encryption methods in use today: secret-key cryptography and public-key cryptography. SET uses both methods in its encryption process (Anon., 1997d:14).

The SET protocol uses cryptography to :

- provide confidentiality of information,
- ensure payment integrity, and
- authenticate both merchants and cardholders (Set Central -RSA Data Security, 1997a:1).

Secret-key cryptography, also known as symmetric cryptography, uses the same key to encrypt and decrypt the message. Therefore, the sender and the recipient must share a secret, namely the key. A well known secret-key cryptographic algorithm is the Data Encryption Standards (DES), which is used by financial institutions to encrypt PINs (Personal identification numbers) (Anon., 1997d:14).

Public-key cryptography, also known as asymmetric cryptography, uses two keys: one key to encrypt the message and the other key to decrypt the message. The two keys are mathematically related so that data encrypted with either key can only be decrypted using the other. Each user has two keys: a public key and a private key. The user distributes the public key. Because of the relationship between the two keys, the user and anyone receiving the public key can be assured that data encrypted with the public key and sent to the user can only be decrypted when the user uses the private key. This assurance is only maintained if the user ensures that the private key is not disclosed to anyone else. Therefore, the key pair should be generated by the user. The best known public-key cryptography algorithm is RSA (named after its inventors Rivest, Shamir, and Adlemman) (Anon., 1997d:15).

Secret-key cryptography is impractical for exchanging messages with a large group of previously unknown correspondents over a public network. For a merchant to conduct transactions securely with millions of Internet subscribers, each consumer would need a distinct key assigned by that merchant and transmitted over a separate, secure channel. On the other hand, by using public-key cryptography, that same merchant could create a

public/private key pair and publish the public key, allowing any consumer to send a secure message to that merchant.

Confidentiality is ensured by the use of message encryption. When two users want to exchange messages securely, each of them transmits one component of their key pair to the other and keeps secret the other component, designated the private key. Because messages encrypted with the public key can only be decrypted using the private key, these messages can be transmitted over an insecure network without fear that an eavesdropper could use the key to read encrypted transmissions.

SET will rely on cryptography to ensure message confidentiality. In SET, message data will be encrypted using a randomly generated symmetric encryption key. This key, in turn, will be encrypted using the message recipient's public key. This is referred to as the "digital" envelope of the message and is sent to the recipient along with the encrypted message itself. After receiving the digital envelope, the recipient decrypts it using his or her private key to obtain the randomly generated symmetric key and then uses the symmetric key to unlock the original message.

To provide the highest degree of protection, it is essential that the programming methods and random number generations algorithms generate keys in a way that ensures that the keys cannot be easily reproduced using information about either the algorithms or the environment in which the keys are generated (Anon., 1997d:16).

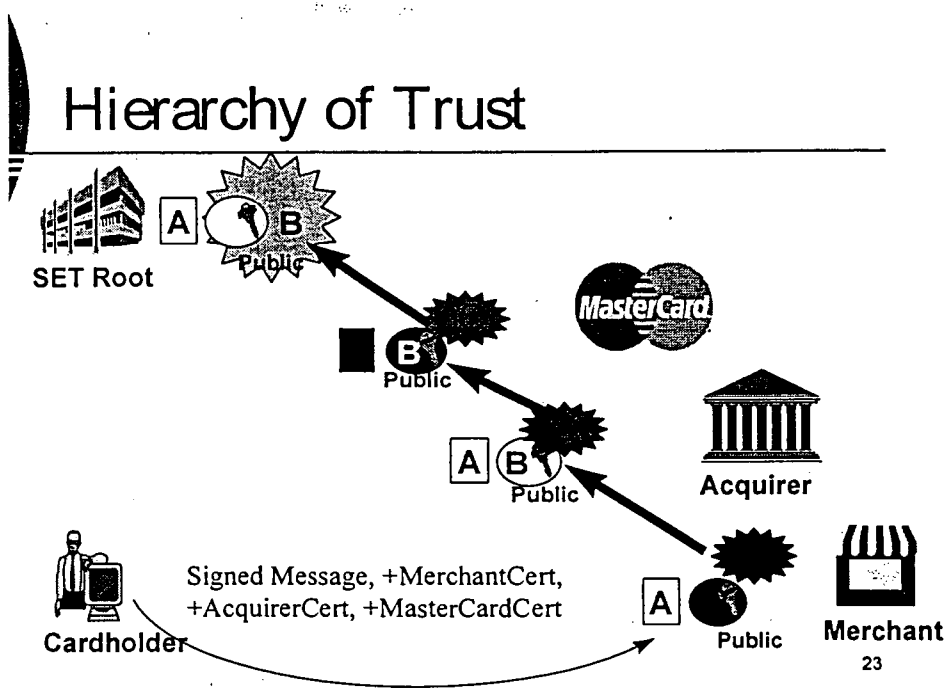

FIGURE 2.2 CERTIFICATES - HIERARCHY OF TRUST (Anon., 1997d:13)

Integrity and authentication are ensured by the use of digital signatures. Because of the mathematical relationship between the public and private keys, data encrypted with either key can only be decrypted wit the other. This allows the sender of a message to encrypt it using the sender's private key. Any recipient can determine that the message came from the sender by decrypting the message using the sender's public key (Anon., 1997d:17).

When combined with message digests, encryption using the private key allows users to digitally sign messages. A message digest is a value generated for a message (or document) that is unique to that message. The algorithm used by SET generates 160-bit message digests. The algorithm is such that changing a single bit in the message will change, on average, half the bit is in the message digest. Roughly, the odds against messages having the same message digest are most rare. It is computationally unfeasible to generate two different messages that have the same message digest. A message digest is generated by passing the message through a one-way cryptographic function; that is,

one that cannot be reversed. When the digest of a message is encrypted using the sender's private key and is appended to the original message, the result is known as the digital signature of the message.

The recipient of the digital signature can be sure that the message really came from the sender. And, because changing even one character in the message changes the message digest in an unpredictable way, the recipient can be sure that the message was not changed after the message digest was generated.
SET uses a distinct public/private key pair to create the digital signature. Thus, each SET participant will possess two asymmetric key pairs: a "key exchange" pair, which is used in the process of encryption and decryption, and a 'signature' pair for the creation and verification of digital signatures. Note that the roles of the public and private keys are reversed in the digital signature process where the private key is used to encrypt (sign) and the public key is used to decrypt (verify the signature) (Anon., 1997d:19).

Authentication is further strengthened by the use of certificates. Before two parties use public-key cryptography to conduct business, each wants to be sure that the other party is authenticated. An alternative to secure transmission of the key is to use a trusted third party to authenticate the fact that the public key belongs to the required person . Such a party is known as a *Certificate Authority (CA).* The Certificate Authority authenticates the person's claim according to its published policies as diagramatically represented in Figure 2.2.

Figure 2.3 is best illustrated using an example, a Certificate Authority could supply certificates that offer a high assurance of personal identity, which may be required for conducting business transactions; this Certificate Authority may require a person to present a driver's license or passport to a notary public before it will issue a certificate. Once the person has provided proof of identity, the Certificate Authority creates a message containing the person's name and public key. This message, known as a certificate, is digitally signed by the Certificate Authority. It contains owner

identification, as well as a copy of one of the owner's public keys ("key exchange" or "signature"). To get the most benefit, the public key of the Certificate Authority should be known to as many people as possible. Thus, by trusting a single key, an entire hierarchy can be established in which one can have a high degree of trust. Because SET participants have two key pairs, they also have two certificates. Both certificates are created and signed at the same time by the Certificate Authority (Anon., 1997d:19).

2.6.3 DUAL SIGNATURES

SET introduces a new application of digital signatures, namely the concept of dual signatures. To understand the need for this new concept, consider the following scenario with Bob and Alice as role players:
Bob wants to send Alice an offer to purchase a piece of property and an authorisation to his bank to transfer the money if Alice accepts the offer, but Bob doesn't want the bank to see the terms of the offer nor does he want Alice to see his account information. Further, Bob wants to link the offer to the transfer so that the money is only transferred if Alice accepts his offer. He accomplishes all of this by digitally signing both messages with a single signature operation that creates a dual signature (Anon.,. 1997d:23).

A dual signature is generated by creating the message digest of both messages, concatenating the two digests together, computing the message digest of the result and encrypting this digest with the signer's private signature key. The signer must include the message digest of the other message in order for the recipient to verify the dual signature. A recipient of either message can check its authenticity by generating the message digest on its copy of the message, concatenating it with the message digest of the other message (as provided by the sender) and computing the message digest of the result. If the newly generated digest matches the decrypted dual signature, the recipient can trust the authenticity of the message.
For example, if Alice accepts Bob's offer, she can send a message to the bank indicating her acceptance and including the message digest of the offer. The bank can verify the

authenticity of Bob's transfer authorisation and ensure that the acceptance is for the same offer by using its digest of the authorisation and the message digest of the offer presented by Alice, to validate the dual signature. Thus the bank can check the authenticity of the offer against the dual signatures, but the bank cannot see the terms of the offer (Anon.,. 1997d:23).

Within SET, dual signatures are used to link an order message sent to the merchant with the payment instructions containing account information sent to the Acquirer. When the merchant sends an authorisation request to the Acquirer, it includes the payment instructions sent to it by the cardholder and the message digest of the order information. The Acquirer uses the message digest from the merchant and computes the message digest of the payment instructions to check the dual signature (Anon., 1997d:23).

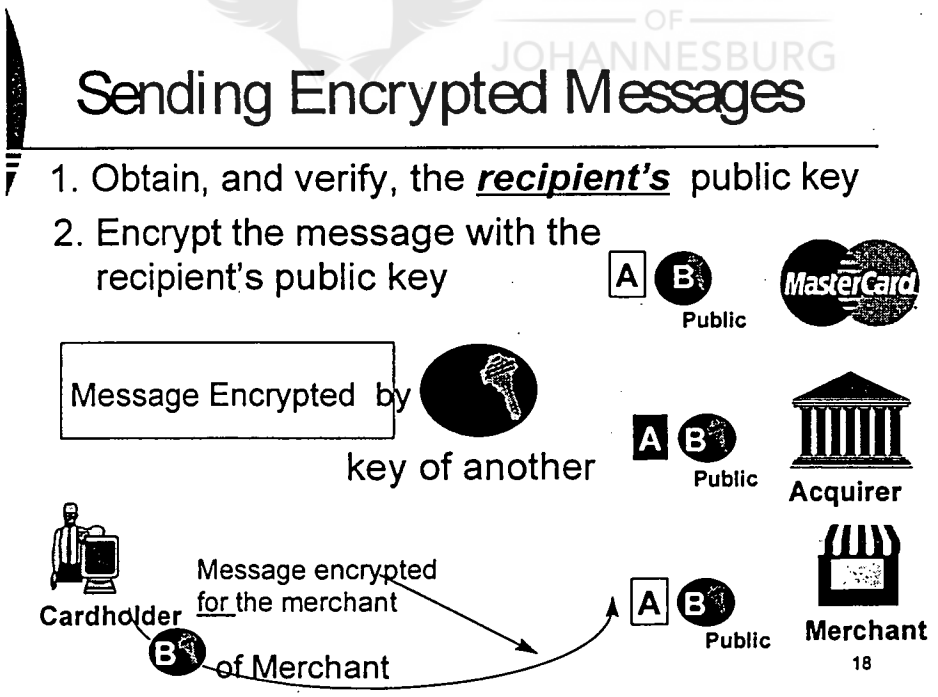

FIGURE 2.3 ENCRYPTED MESSAGES (Anon., 1997d:18)

The primary motivation for the payment card brands to provide specifications for secure payments are to:

- encourage the payment card community to take a leadership position in establishing a secure payment specification and, in so doing, to avoid costs associated with future reconciliation of implemented approaches;
- respect and preserve the relationship between merchants and acquirers and between cardholders and issuers;
- facilitate rapid development of the marketplace;
- respond quickly to the needs of the financial services market; and
- protect the integrity of payment card brands (Anon., 1997d:4).

The objectives of payment security are to:

- authenticate cardholders, merchants, and acquirers;
- provide confidentiality of payment data;
- preserve the integrity of payment data; and
- define the algorithms and protocols necessary for these security services.

The objectives of interoperability are to:

- clearly define detailed information to ensure that applications developed by various vendors will interoperate;
- create and support an open payment card standard;
- define exportable technology throughout, to encourage globally interoperable software;
- ensure compatibility with and acceptance by appropriate standard bodies; and
- allow for implementation on any combination of hardware and software platforms, such as PowerPC, Intel, Sparc, UNIX, MS-Dos, OS/2, Windows, Macintosh.

The objectives of market acceptance are to:

- achieve global acceptance via ease of implementation and minimal impact on merchant and cardholder end users;

- allow for "bolt-on" implementation of the payment protocol to existing client applications;
- minimize change to the relationship between acquirers and merchants, and cardholders and issuers;
- allow for minimal impact to existing merchant, acquirer, and payment system applications and infrastructure; and
- provide an efficient protocol for financial institutions(Anon., 1997d:4).

2.6.4 CERTIFICATE ISSUANCE

Just as important as the issue of confidentiality is authentication. One way of verifying digital identities is for every user to maintain a personal list of the public keys of those people or businesses with which he or she interacts, and this model is known as the "web of trust". Each person individually decides which other signers to trust. A key that has a signature from a trusted signer is accepted as validated. On a global scale it is difficult, if not impossible, for each user to validate the identity of the entity with which trusted third parties can perform independant verification, or certification, of identities. In the evolving framework of electronic commerce, these trusted parties have become known as certification authorities, and the digital documents that are issued are called certificates.

2.6.6.1 Trusted Third Parties

A digital certificate binds an identity to a pair of cryptographic keys used for encryption and digital signatures. Certificates allow verification of the claim that a given public key does in fact belong to a given individual, and they help prevent someone from using a phony key to impersonate someone else. If a driver's license is used for identification in writing cheques, the merchants accept this because they trust the organisation that issued it. The same holds true for certificates. Certificates are issued by a certification authority

(CA), which can be any trusted central administration willing to vouch for the identities of those parties to whom it issues certificates (Klur, 1996:29).

2.6.6.2 Levels of Assurance

Implicit in any certification authority framework is the fact that the participants must rust the CA. The CA must be a widely recognised and trusted organisation. Natural candidates for this job would be well-established high-technology firms, banks or audit firms. The CA should comply with the following:

- be technically valid; and
- make it known how it verifies the identity of the individual requesting a certificate.

There is a cost associated with background checks, interviewing individuals, etc., and therefore the more "trusted" certificates will also be more expensive.
Multiple digital certificates can be attached to a message or transaction, forming a certificate chain where each certificate attests to the authenticity of the previous certificate. The top-level certification authority must be independently known and trusted by the recipient. This is known as a "hierarchy of trust".

Key revocation is just as important as key issuance. Certificate revocation is required in the following circumstances:

- where the private key of a certifying authority has been compromised;
- where the private half of a certified public key has been compromised; or
- where a holder of a certificate is no longer authorised to perform a certain function.

Similar risks as identified in 2.2.1 would be applicable (Klur, 1996:28).

2.6.6.3 Cardholder Certificates

Cardholder certificates function as an electronic representation of the payment card. Because they are digitally signed by a financial institution, they cannot be altered by a

third party and can only be generated by a financial institution. A cardholder certificate does not contain the account number and expiration date. Instead the account information and a secret value known only to the cardholder's software are encoded using a one-way hashing algorithm. If the account number, expiration date, and the secret value are known, the link to the certificate can be proven, but the information cannot be derived by looking at the certificate. Within the SET protocol, the cardholder supplies the account information and secret value to the payment gateway where the link is verified.
A certificate is only issued to the cardholder once the cardholder's issuing financial institution has approved it. By requesting a certificate, a cardholder has indicated the intent to perform commerce via electronic means. This certificate is transmitted to merchants with purchase requests and encrypted payment instructions. Upon receipt of the cardholder's certificate, a merchant can be assured, at a minimum, that the account number has been validated by the card-issuing financial institution or its agent.

2.6.6.4 Merchant Certificates

Merchant certificates function as an electronic substitute for the payment brand decal that appears in the store window - the decal itself is a representation that the merchant has a relationship with a financial institution allowing it to accept the payment card brand. Because they are digitally signed by the merchants financial institution, merchant certificates cannot be altered by a third party and can only be generated by a financial institution.
These certificates are approved by the acquiring financial institution and provide assurance that the merchant holds a valid agreement with an Acquirer. A merchant must have at least one pair of certificates to participate in the SET environment, but there may be multiple certificate pairs per merchant. A merchant will have a pair of certificates for each payment card brand that it accepts (Anon., 1997d:25).

2.6.6.5 Payment Gateway Certificates

Payment gateway certificates are obtained by acquirers or their processors for the systems that process the authorisation and capture messages. The gateway's encryption key, which the cardholder obtains from this certificate, is used to protect the cardholder's account information.
Payment gateway certificates are issued to the Acquirer by the payment brand.

2.6.6.6 Acquirer Certificates

An acquirer must have certificates in order to operate a Certificate Authority that can accept and process certificate requests directly from merchants over public and private networks. Those acquirers that choose to have the payment card brand process certificate requests on their behalf will not require certificates because they are not processing SET messages. Acquirers receive their certificates from the payment card brand.

2.6.6.7 Issuer Certificates

An Issuer must have certificates in order to operate a Certificate Authority that can accept and process certificate requests directly from cardholders over public and private networks. Those Issuers that choose to have the payment card brand process certificate requests on their behalf will not require certificates because they are not processing SET messages. Issuers receive their certificates from the payment card brand (Anon., 1997d:26).

2.7 CONCLUSION

There are numerous security risks relating to commercial transactions on the Internet.

No Internet security model provides perfect protection against the risks identified :

- confidentiality;
- authentication;
- data integrity;
- nonrepudiation; and
- access to services.

However, the implementation of SET as an open, free, non-competitive and interoperable standard does address the above issues to an extent.

In the writer's opinion, the objective of the literature survey was achieved. Chapter 3 will cover an empirical study of SET relevant institutions.

CHAPTER 3 - EMPIRICAL STUDY

The literature survey on validity of transactions using SET is set out under the following headings:

3.1 OBJECTIVE

3.2 NATURE OF EMPIRICAL STUDY

3.3 SCOPE, LIMITATIONS AND EXCLUSIONS

3.4 BACKGROUND

3.5 RESULTS OF FIELD STUDY

3.6 CONCLUSION

3.1 OBJECTIVE

The objective of this chapter is to supplement the theoretical research presented with some authoritative views on SET and its implementation thus far.

3.2 NATURE OF EMPIRICAL STUDY

To ensure credibility and acceptance of the findings and proposal of this short dissertation, it is essential that the underlying concepts be based on authoritative views and be generally accepted among auditing professionals. Theory based on an individual's experience without taking generally accepted professional views into account, may be subject to personal bias. Other factors which may introduce bias are the individual's background and the absence of formal research. To avoid these problems, references have been restricted to those published by auditors and professional auditor's bodies. The main categories of authors/publishers are:

- Experts i.r.o. SET; and
- Mastercard.

The reasons for choosing these authors/publishers are:

- They represent between them most of the internationally accepted view of SET;
- The emphasis on auditor-related references provide more and better background for finding risks relevant to the auditor involved in SET; and
- In total, they represent a properly balanced view of SET.

3.3 SCOPE, LIMITATIONS AND EXCLUSIONS

South African institutions that are in the process of testing and accessing the viability and security surrounding SET are primarily the banking institutions, and therefore a questionnaire was designed to be directed to the above sector with SET specific questions to be answered.

Four of the major banks in South Africa were approached, viz. Standard Bank, Absa, Nedbank and FNB. Although a population of four was chosen, the response has still been poor. After setting up meetings, the "Heads of Security" informed me that additional authorisation was required to answer all the questions.

A great deal of preparatory work has been done to ensure that the short disertation is based on available and sound theory and the limitations and exclusions imposed do not detract from the overall objective of this dissertation, in fact they concentrate on those issues which are relevant to a short dissertation of this nature.

Some of the reasons for poor responses can be attributed to:

- The banking institutions want to maintain a high level of security without security breaches;
- Due to the competitive environment in which the industry operates, all information is confidential;
- SET will be fully implemented within months, after which I have been invited to call again; and
- Due to the sample size, the belief is that bank-specific information would be used against them to its competitors' advantage.

The questionnaire should be viewed as an internal control framework to assess the adequacy of an organisation's control environment.

The method of research:

- Obtained contact numbers for relevant people eg. Head of Internet Security;
- Telephonically introduced myself and my objectives;
- Set up personal interviews covering the questionnaire;
- Conducted the interviews; and
- Analytically compared the results.

The questionnaire to the banking institutions was structured as follows:

PRIVATE AND CONFIDENTIAL

SET QUESTIONNAIRE

PURPOSE : to determine the current views/trends on the implementation of SET in the banking sector.

1. What percentage of your business is made up of:
   a. Credit card transactions; and
   b. Internet banking.

2. What is the anticipated growth in these areas:
   a. Credit card transactions; and
   b. Internet banking.

3. Has your organisation been certified as being SET compliant?

4. How does one become SET compliant?

5. Which stage of implemenation of SET is your organisation in eg. pilot testing, etc.?

6. How long does it generally take to have SET up and running?

7. Does your firewall monitor and record "hits" taken (both successful and unsuccessful)?

8. What procedures does SET provide to ensure the validity of transactions (acquirer certificate, merchant certificate, payment gateway certificate, crytographic techniques)?

9. What compensating controls are in place to ensure the validity of transactions?

10. Have there been any reported cases of credit card fraud?

11. Discuss problems experienced with SET and what improvements can be recommended?

3.4 BACKGROUND

SET is a relatively new subject with no publications being made to-date. The result has been a fair amount of Internet browsing and communications with Mastercard personnel in New York and attendance at Technology forums to gather information and develop contact people for future purposes.

3.5 RESULTS OF FIELD STUDY

Questions 1a & 2 a (Percentage of current and anticipated growth in credit cards)

These are the predominant views expressed of the respondents:

Although there will not be a significant increase in the number of credit cards being issued because of the South Afican economy, there should be an increase in the number of credit cards transactions processed due to the availability/accessibility of services.

Question1b and 2 b (Percentage of current and anticipated growth in Internet banking)

The respondents did not want to comment because it was a strategic decision which could not be revealed.

Question 3 (SET compliance certificate)

Some of the organisations were in the process of becoming SET compliant, and others regarded the question to be confidential. Further information could be obtained in 1998.

Question 4 (Procedure on becoming SET compliant)

All of the organisations referred to the registrations requirements as per Mastercard/Visa on the Internet, and this was the approach followed by all.

Question 5 (Stages of SET implementation)

This information was regarded as confidential and sensitive at the moment by all respondents.

Question 6 (Time-frame to implement SET)

Respondents indicated that this was dependant on the organisation and their strategic planning.

Question 7 (Firewall monitoring)

All of the respondents said that they indeed had firewalls within their architecture. The positioning of the firewall was regarded as sensitive information.

Question 8 (SET procedures to validate transactions)

Some of the respondents mentioned the Certification Authority/Hierarchy of Trust that was an essential element of SET, yet others regarded the informationto be confidential. Special permission was required for providing this information.

Question 9 (Compensating controls)

No information was forthcoming, since this was perceived as providing inside information on how to "override the system". This was also indicated to be strategic and confidential information.

Question 10 (Reported cases of credit card fraud)

Some of the respondents indicated that there have been many reported frauds. However, these were due to stolen/lost credit cards, and not to credit card numbers being "picked up" from an open network.
Others regarded this as sensitive information.

Question 11 (Recommendations to improve SET)

Many respondents will have more information in 1998.

To attempt to perform a comparison on the above responses would be fruitless at this stage, however this could be useful to use as a foundation for future research.

3.6 CONCLUSION

Due to the poor responses received in the attempted empirical study as well as the current positioning of SET in South Africa and world wide, the questionnaire can be used to assess the adequacy of controls. However, the results of the survey should not be relied upon, instead it is certain that further research has to be be conducted by technical and auditing professionals, since this is a very controversial issue with much value that can be added.

CHAPTER 4 - COMPILATION OF AN AUDIT PROGRAMME

In Chapter 1, it has been seen that the objective of this short dissertation is to develop an audit programme for auditing the validity of transactions using SET protocols. It has been concluded in the literature survey that SET has not been evaluated for auditing purposes as yet. The information provided by the literature survey has to be used to develop this audit programme. That is the objective of this chapter. The development of such an audit programme is described in the following sections:

4.1 INTRODUCTION

4.2 OVERVIEW OF AN AUDIT MODEL

4.3 AUDIT PROGRAMME : AUDITING THE VALIDITY OF TRANSACTIONS USING SET PROTOCOLS

4.4 CONCLUSION

4.1 INTRODUCTION

The high level risks of Internet security relating to credit card transactions have been discussed in chapter 2. The control measures necessary to cover the lack of control within the TCP/IP suite have also been addressed. In chapter 3 a questionnaire was developed to be used as a Control Framework to assess the adequacy of controls. These chapters were used as the basis in developing an audit programme for validating SET transactions.

4.2 OVERVIEW OF AN AUDIT MODEL

In order to illustrate the purpose of the audit programme in the audit process, an outline of an audit model has been set out in Table 4.1.

Phase of the audit process	Aspects covered	Visible outputs
• Planning	- Understand the entity - Survey and identify matters of significance - Audit planning	- Analysis and survey plan - Audit plan
• Detailed Examination	- Network and Internet security	- Audit programme - Audit files
• Reporting	- Report on the audit	- Draft and final reports

TABLE 4.1 AUDIT MODEL FOR VALIDATING TRANSACTIONS USING SET PROTOCOLS

For the purposes of this short dissertation, only the detailed examination phase is addressed. The planning phase will encompass the preliminary survey, set up interviews with the auditees and general gathering of information and identification of key risks. Reporting of audit findings will take a draft and final format to management. In addition, only the audit objective of validity will be considered in developing this audit programme. The following audit programme was compiled as a guideline to evaluate the adequacy and effectiveness of controls over the implementation of SET for electronic transactions.

4.3 AUDIT PROGRAMME FOR AUDITING THE VALIDITY OF TRANSACTIONS USING SET PROTOCOLS

DESCRIPTION OF AUDIT CONTROL	YES	NO	WP REF	REFERENCE TO CHAPTERS 2 AND 3
1. Standards for password creation and 2. maintenance are documented and communicated.				2.4
3. Passwords are at least six characters long and cannot be easily compromised.				2.4
4. Passwords are changed at least once per month.				2.4
5. Sensitive files are transmitted using an encryption technique.				2.5

6. Business and credit card numbers use a secured browser and protocol.				2.6.1
7. User ids and passwords are encrypted for sensitive transmissions.				2.5
8. Electronic mail is encrypted by using Privacy Enhanced Mail.				2.
9. Authentication is required for sensitive transmissions.				2.5; 2.6.1
10. Firewalls are in place and allow packet and protocol access by exception only.				2.4
11. Routers restrict protocols to authorised ports and hosts.				2.4
12. Certification for the Web site has been obtained.				2.4
13. Links do not access confidential information.				2.6.4
14. Secured browsers are required for business transactions.				2.6.3
15. Web site updates are tested for security or certification circumvention.				2.6.3; 2.6.6

16. All transmissions are logged by firewall, proxy server, or other software.				2.4; 2.6.1
17. A system or security administrator reviews transmission logs and resolves and notes problems.				2.4
18. Modems, routers, firewall hardware, phone lines, and port connections are physically secure.				2.4; 2.6.1
19. Operating system, usage system, and network system software are physically secure.				2.4
20. Usage information and security table information should be backed up regularly.				2.4; 2.6.1
21. Internet security policy has been established and kept up-to-date..				2.4; 2.6.6
22. Maintenance of logs, recording user-id, sign-on dates and times, session duration, etc.				2.4; 2.6.1
23. Security administrator to regularly run software such as enhanced logging and real-time alarms to immediately detect hacker or insider intrusions.				2.4

24. Exception reports indicating the number of "hits", successful and unsuccessful attempts should be reviewed by management.				2.4; 2.6.1
25. System logs should be secured.				2.4; 2.6.1
26. The Certificate Authority process as per operating procedure should be adhered to.				2.6.6
27. The certificate server is physically and logically secured.				2.6.6
28. Dual signatures and message digests are utilised to ensure data integrity.				2.6.4; 2.6.5

TABLE 4.2 AUDIT PROGRAMME TO VALIDATE TRANSACTIONS USING SET PROTOCOLS

4.4 CONCLUSION

The audit programme has been compiled for auditing the validity of transactions using the SET protocol. The audit programme should be viewed as a guide with enhancements to be made depending on the nature of the business involved.

The application of this audit programme could also assist the auditor in adding significant value within an organisation, that is venturing into "untested waters".

CHAPTER 5 - CONCLUSION

The objective of this short dissertation has been met, that is to help the auditor to audit the validity of transactions using SET protocols. The understanding of the key participants and components of SET is imperative for the efficient audit thereof.

The main problem identifed, has been the need to develop an open standard to conduct secure electronic transactions over the Internet. Although firewalls have been used to secure Internet connectivity, consumers were hesitant to transact or "make available" sensitive and confidential information like account numbers and account balances. SET has attempted to address the loopholes or risks that have been previously identified with its non-competitive, free and interoperable standard.

The model developed in Chapter 4 is in no way a replacement for good Internet commercial security, but can assist the auditor in determining the risk associated with commercial transactions on the Internet and consequently the audit approach that should be followed. Client service (where auditors also give business advice and not only do the compliance audit for a client), can be maximised by using this programme.

It opens new fields for academic research in the areas of electronic transactions including E-Cash, E-Debit, Digital Cash, Smart cards, etc. This short dissertation has focused specifically on SET and the validity of the transactions, the accuracy, completeness and maintenance of transactions are potential areas of research. An audit programme for the evaluation of a sucrity approach to commercial transactions could be developed. This security approach should include security policies, procedures, standards and all security components implemented.

BIBLIOGRAPHY

1. ANON. 1997a: Set Central -RSA Data Security, [online]. Available URL address: http://www.rsa.com/set.

2. ANON. 1997b: Paying by Credit Card - Real World and Online, [online]. Available URL address: http://www.virtualschool.edu/mon/E.

3. ANON. 1997c: Mastercard and Visa select Terisa, [online]. Available URL address: http://www.ramresearch.com/crdflash.

4. ANON. 1997d: Book1: Business description. [online]. Available URL address: http://www.mastercard.com.

5. BHIMANI, A 1996: Securing the Commercial Internet, Communications of the ACM, 39(6), June 1996:29-35.

6. KLUR, D 1996: Certification Authorities and Electronic Commerce. IS Audit and Control Journal, Vol 4, 1996:29-31.

7. QUELCH, JA & KLEIN, LR 1996: The Internet and International Marketing. Sloan Management Review, 37(3), 1996:

8. PAYNE, J & POOL, D 1995: Forging Ahead. Internet World, 6(5) 1995: 27.

9. TIBALDEO, G & BUBEN, D 1996: Secure Electronic Transactions. IS Audit and Control Journal, Vol 4, 1996: 19.

10. SET SPECIFICATION AGENDA (1st:1997: Kuala Lumpur).