e-Everything: e-Commerce, e-Government, e-Household, e-Democracy

14th Bled Electronic Commerce Conference

Bled, Slovenia, June 25 - 26, 2001

The Integration of SET in Australian Based Internet Payment System Products: A System Developer's Perspective

Mustafa A. Ally

University of Southern Queensland, Faculty of Business and Commerce
Department of Information Systems
West Street, Toowoomba 4350, Queensland, Australia
Mustafa.Ally@usq.edu.au

Abstract

The SET (Secure Electronic Transactions) protocol was designed as an open industry standard for the secure transmission of payment information over private and public networks. Anecdotal evidence suggested that SET had been slow to get off the mark in Australia for several different reasons, notably the absence of software products, its limited functionality, and cost of implementation. This exploratory study sets out, firstly, to identify the reasons for this reluctance to adopt and implement SET by a variety of Internet Payment System (IPS) developers promoting their products in the Australian e-Commerce market. This begs the question as to the level of consideration given to security and other payment system issues in these systems. To this end, the paper then analyses the alternate tools and services these vendors have utilized (if any) in order to comply with the established payment security requirements of confidentiality, authentication, integrity and non-repudiation that SET was designed to address.

Keywords: *SET, Internet Payment Systems, Security*

1. Introduction

The growing activity of business over the Internet has increased the demand for an open global framework for electronic commerce with secure payment systems, seen as a major barrier to the more widespread acceptance of e-Commerce. The main electronic payment methods for e-commerce are modeled after the paper world, such as electronic cash, electronic cheques and electronic payment cards [17]. This

paper focuses on the credit-card payment systems developed for use over the Internet and, in particular, studies the role (or absence) of SET in these products.

It deals with the question as to what has been achieved thus far, in particular, in the Australian market, to address the demand for a secure, cost-effective on-line payment card processing system. To this end the SET protocol, designed primarily to address such issues, is used both as a point of reference and well as a benchmark for secure payments over the Internet.

The first section of this paper describes the need for a secure payment infrastructure in the context of the Internet. It reviews the security requirements for safely conducting payment transactions over the Internet, the main difficulties that have arisen and the role SET has played in their resolution. The second section describes the operational aspects of credit card systems, and in specific, outlines the role of SSL and SET in this regard. This follows with a description of the research objectives and the methods of data collection employed in this exploratory study. Finally, a discussion of the preliminary responses to the study is made against the issues raised in SET's business plan. The paper concludes with a recommendation for further research in this area and a review of the key issues.

2. The Scope of the Study

This paper identifies those issues specifically related to the use of credit card payment systems over the Internet. In analyzing a selection of payment systems in the Australian market, the products are viewed as black boxes, without commenting on the technical details and merits of each. Emphasis is placed on the authorization and capture process and the fundamental security services of confidentiality, authentication, integrity and privacy as supported by them. It does not evaluate them on other value-added services that they may also be providing. The purpose of the service definitions is to provide a description of the different approaches taken (or the lack thereof) to satisfy these requirements.

3. Background

In Australia the number of online shoppers has increased by 600 per cent in the last three years, according to Red Sheriff research. Currently 5.21 million Internet users in Australia make online purchases, according to IDC. Sixty per cent of all online merchants in Australia currently use electronic payment solutions [9]. In its Australian Online Shopping report, www.consult.com.au estimated domestic online shopping would be worth A$10.9 billion or 5% of total retail spending by the end of 2002. Australia is number three behind the US and Canada in terms of the uptake of online transactions [13].

To become an active market in goods and services the Internet must overcome a fundamental hurdle: a way must be devised for buyers and sellers to exchange payment securely and conveniently over the Internet [12]. Several studies referred to by [10] have identified the factors impeding the growth of Internet based

commerce. One of these factors is the payment component. The issues of trust and transaction security have impacted on the willingness of consumers to make electronic commerce purchases, with a reported 65% reluctant to purchase goods online and to submit their payment details over the Internet. These concerns pose a major hurdle to consumer acceptance of electronic commerce – of the total number of consumers who browse Internet stores, only around 2.7% actually make a purchase. These statistics are quoted by [20] from independent research companies, in particular, ActiveMedia Research and the Intermarket Group.

The vast number of international retail payments on the Internet are made using credit cards, usually involving the safety features coming with standard browsers (e.g. SSL), but also completely unencoded or by such means as fax or the telephone. With the introduction of SET and its ability to create a trusted environment through the authentication of all the parties concerned in the payment transaction, it should have been safe to assume that these concerns would have been largely eliminated. However, there has been a degree of reluctance on the part of many card payment product developers and banks to readily adopt the protocol. The report on electronic payment systems in European countries states that while there is interest from the side of the credit card organisations and some merchants in the SET protocol, adoption has been very slow and that it is presently difficult to convince customers of its benefits [4].

4. The Need for a Secure Payment Infrastructure

The security of a payment system means an assurance of the correctness of the payment system provided by technical measures and banking procedures [17]. Studies of several surveys on Internet usage indicate that security concerns were an important obstacle to on-line shopping. In a World Research Survey, 21 per cent of respondents who had not bought online cited fear of hackers as their reason [21]. The survey also reported that another 12 per cent cited distrust of Internet companies or a fear that money or merchandise would be lost. A similar survey found that 15 per cent of its respondents feared misuse of information by the intended recipient while 7 per cent feared hackers [6].

Electronic commerce is in an embryonic stage, and technology and market dynamics are still casting its basic shape. This is especially true for the business-to-consumer segment, where concerns about security of payment, potentially fraudulent merchants, privacy of personal data, and difficulty and expense in accessing e-commerce merchants affect its growth potential. These issues represent significant policy challenges [14].

The openness, global reach, and lack of physical clues that are inherent characteristics of e-Commerce also make it vulnerable to fraud and thus increase certain costs for e-Commerce merchants as compared to traditional stores. While a variety of payment systems are being tested, the credit card is the dominant online payment so far, and e-Commerce merchants are exposed to potentially higher levels of fraud resulting from stolen cards or illegally obtained card numbers.

Because of the rule on distance retail (if the credit card is not physically present, the merchant is liable for all the costs associated with the fraud even if the bank has authorized the transaction), e-Commerce merchants could face added costs because of their exposure to fraud. In common with all other electronic information processing systems, payment systems are prone to disruption by people exploiting the systems' innate vulnerabilities. All financial systems attract fraudsters and embezzlers [16].

To pursue the objective of safety in a payment system, it is necessary first to identify and understand how risks of various types may arise or be transmitted within the system and to determine where they are borne. Once these risks are properly analyzed and assessed, appropriate mechanisms must be devised to monitor, manage and control them [7].

The next section identifies and explains these threats.

5. Basic Security Requirements of a Payment System

The OECD Guidelines for consumer protection in the context of electronic commerce and the payment process call for consumers to be provided with easy-to-use, secure payment mechanisms and information on the level of security such mechanisms afford [14].

This section defines the requirements for a secure payment system and highlights the strategy adopted by the SET protocol to deal with them, where such strategies are in place.

Privacy

It is essential in any payment system that the privacy of the consumer is respected.

One likely opportunity for compromising a payment system is in the instance where a merchant collects the client's payment instructions (credit card numbers, etc) and holds the details in open databases, albeit transitorily in some cases. This leaves these details vulnerable to attack by anyone who can gain access to the merchant's system [16]. Using this information, hackers can create counterfeit cards and fraudulent transactions – a major security concern.

By including the bank in the purchasing triangle, SET effectively removes the need for credit card information to travel to the merchant. Encrypted data fields that are sent via the merchant to the acquirer can only be decrypted by the payment gateway. This also ensures that the cardholder is dealing with a valid, payment card-approved merchant.

Non-repudiation

Non-repudiation means that a party cannot falsely deny later that a certain transaction took place. One method to achieve non-repudiation is the use of digital signatures, which, when verified against a public key serves as proof that the signed transaction originated from someone knowing the corresponding secret (private) key. About half of all chargebacks to merchants in the direct marketing industry

occur when cardholders repudiate transaction, or claim that they did not order whatever they were charged for [5].

SET, per se, does not provide non-repudiation. It permits non-repudiation via the rules and policies of the individual card brand implementations [18].

Integrity

A merchant must be assured that the order he/she receives is what the cardholder submitted. Mechanisms to overcome the risk of transaction information being altered in transit should be employed.

SET provides integrity by employing one-way cryptographic hashing algorithms and digital signatures to ensure that a message was not modified in transit.

Authentication

Authentication is the process that seeks to validate identity or to prove the integrity of information. The anonymity of Internet shopping means that cardholders cannot know for sure which merchant they are dealing with or whether the merchant is properly authorised to handle payment card transaction. Similarly, merchants have no way of verifying whether the cardholder is in possession of a valid payment card or has the authority to be using that card.

SET addresses these concerns by using digital signatures and digital certificates to authenticate the banking relationships of cardholders and merchants [20].

Confidentiality

A payment system should be capable of maintaining public confidence by ensuring customer privacy. The need for confidentiality prescribes that data cannot be interpreted by anybody other than the sending or receiving parties. Confidentiality in this context means restriction of the knowledge about various pieces of information related to a transaction: the identity of the payer/payee, purchase content, amount, and so on [2]. The confidentiality of payment data is presently protected through a regime of data encryption.

SET provides confidentiality by employing both asymmetric and symmetric data encryption algorithms to protect financial information from eavesdroppers.

Certificates and Certificate Management

The issues of trust and transaction security are amongst the major challenges being posed in e-Commerce today. A trusted environment will accelerate the consumer's willingness to make online purchases. For e-Commerce, the only known feasible method to do this is through the use of digital certificates and signatures [8]. When digital signatures are used, a public key infrastructure (PKI) is required. The most common way of key distribution makes use of certificates, which are issued by a trusted third part (mostly using the ISO X.509 certificate standard).

In the SET environment, there is a hierarchy of Certificate Authorities. The SET protocol specifies a method of entity authentication referred to as trust chaining. This method entails the exchange of digital certificates and verification of the public keys by validating the digital signatures of the issuing CA [19].

6. Barriers to the Establishment of a Secure Infrastructure

While e-Commerce can dramatically reduce production costs, it does not really offer a "friction-free" environment. Rather, owing to new costs and new processes associated with establishing trust and reducing the risks inherent in this type of activity, new intermediaries and infrastructure are required. A few of the inhibitors are discussed here.

Public Key Infrastructure (PKI)

One of the most important security mechanisms in SET is the use of digital signatures. This will require a full understanding by the client as the security of end-user private keys with software poses a real problem. In addition to not being portable, they can be stolen off a computer easily. Anyone in possession of the private key) or a copy of it, can make a digital signature [15]. Although VeriSign's NetSure Protection Plan provides a limited warranty protection against the loss, theft, modification, or unauthorized access to the subscriber's private key, it does assume that the subscriber has taken reasonable precautions to prevent loss or unauthorized use of the private key and that he/she uses computer systems that are reasonably secure from intrusion or misuse [23].

Wallets

To enable a SET transaction, a consumer needs a SET enabled electronic wallet. The wallet is a software application, which is either held on a cardholder's computer (the so called, "fat wallet") or is managed on his/her behalf on a secure server ("thin wallet"). It stores key information required for the transaction such as the payment brand account number and expiration date and the cardholder's SET certificate.

The use of a SET wallet introduces several barriers to the adoption of SET as a protocol. Amongst the limitations described in [1] are the cumbersome setup process, lack of cardholder mobility between computers, recovery from hardware failure, etc.

Performance and Costs

Payment systems consume substantial resources. The [7] consultative report, in defining its public policy on payment systems, states as one of its objectives that the designers and operators of payment systems be conscious of the resource costs of their systems and the charges they will need to pass on to users if resources are to be used efficiently. Cost constraints are likely to require choices to be made about a system's design, which will have an impact on the system's functionality and safety. The functionality required will vary from one system to another according to the demands of participants and users. Payment systems must always achieve a high level of safety appropriate to their potential for triggering or transmitting systemic risk. ***Little, however, would be gained if a payment system were designed with such extensive safety features that it became so difficult, slow or costly to use that no one was prepared to do so.*** It must be remembered that the use of digital certificates and the authentication process can make a system about three times slower (20 to 30) seconds slower than traditional transaction processing.

7. Operational Credit Card Payment Systems

This section gives a brief overview on operational credit-card payment systems and focuses on the two protocols affording various degrees of security support.

The process of using credit-card payments over the Internet is similar to the process of using the credit card in conventional sales transactions: there is a **purchase request** and **response** between the buyer (payer) and merchant (payee) and there is an **authorization** and a **capture request-response** pair between the merchant and acquirer [17]. In the case of SET a payment gateway is also involved.

SSL and SET are the two leading protocols in use today for securing the online purchasing process.

Secure Socket Layer (SSL) Encryption

The dominant cryptographic protocol in current e-Commerce deployment is undoubtedly SSL (now in the final stages of IEFT standardization as TLS). In its current version, SSL allows connections to be established in which both parties are authenticated to each other, in which only the server is authenticated, or entirely anonymous connections. SSL/TLS provide an effective means for securing the channel. It is widely implemented in the major browsers and servers

Confidentiality and Integrity: As all traffic is encrypted and hashed, SSL provides a high degree confidentiality and integrity. Many product manufacturers advertise their use of 56-bit or 128-bit DES encryption and 1024-bit public keys. What should be remembered is that the length of the keys actually used will often depend on the client's browser. If, as is commonly the case, it is restricted to 40-bit DES and 512-bit public key, the encryption used will be at that level. Consideration should be given as to whether the lower level of security this offers is sufficient for the purpose.

Authentication & Non-Repudiation: SSL can provide server and client authentication through the deployment of digital certificates issued from within a PKI and stored in the client browser. There are several disadvantages to this model [3], namely:

- The digital certificates are attached to the software and not to the end-user. Therefore there is the absence of the concept of a digital signature that is bound to the end-user and as a consequence it is not feasible to provide an authentication framework for multiple users of a single [PC] browser.
- The certificate in the browser is not easily portable, for instance for use at home and in the office.
- Authentication of the buyer and non-repudiation are not ensured. The communication over the Internet is limited to the transfer of data between buyer and merchant; the acquiring bank does not communicate over the Internet (no multi-party protocol) [17]

SET

Secure Electronic Transactions (SET) specifies a technical protocol for securing credit-card transactions over the Internet using cryptography and a public key infrastructure.

SET describes a multi-party protocol that establishes a link between the buyer, merchant and the payment gateway of the acquiring bank. The payment gateway connects the Internet to the existing traditional payment infrastructure. The gateway will either be run by the acquiring bank or by a company contracted by the acquiring bank to do so on their behalf. In addition to encrypting information for privacy and security, SET also verifies the identity of each party in an online transaction. For merchants, this means that the person making the transaction is certified as the cardholder and is authorised to make the payment, and that there are sufficient funds available. For consumers, it means that the merchant has been certified as a real merchant, overcoming the risk of paying for a non-existent product.

In contrast with SSL/TLS, the SET protocol, designed by the bankcard associations (VISA and MasterCard), deals only with the secure transmission of payment instructions. The credentials (digital certificates) used to authenticate the parties are not intended to authenticate their holders outside of this narrow scope. The SET protocol also relieves the trader of the burden of maintaining the confidentiality of card numbers and associated details: it is a three-party protocol which includes the merchant's card processor (the merchant's acquiring bank) as well as the cardholder and the merchant, with the card number being encrypted in the acquiring bank's key rather than the merchant's, and the merchant receiving an authenticated 'authorization' or 'denial' from the bank, along with a transaction-specific identifier against which payment can be claimed [24].

The SET Business Plan

Card issuers defined seven major business requirements for SET [11]. According to the SET Business Plan, SET should

- Provide confidentiality of payment information and enable confidentiality of the order (merchandise) information that is transmitted along with the order's payment information
- Ensure integrity for 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 of an electronic commerce transaction
- Ensure the creation of a protocol that is neither dependent on transport security mechanisms nor prevents their use

- Facilitate and encourage interoperability across software and network providers

8. Research Objectives and Methodology

The research described in this paper is exploratory in nature, and designed to elicit a preliminary catalogue of issues related to the development of secure payment systems.

The study began with the broad research question: "What, in your opinion, are the reasons for the slow uptake of SET in Australia?" Working with data collected from these sources the analysis is guided by the following research questions:

- What are the infrastructural deficiencies standing in the way of the widespread deployment of SET in local Internet payment products?
- What factors inhibit the support for SET?
- How do local products contend with the issues of confidentiality, authentication, integrity, non-repudiation, and interoperability?

While payment systems are an essential component of most e-Commerce solutions today, the number of players developing such systems and providing this niche service is somewhat limited. Given the exploratory, interpretive nature of this research, it was determined that the data for this study would be derived from three sources. A sample of 10 developers was selected from a list of 34 Internet Payment Providers and Payment System Developers to participate in this exploratory study. All of these providers and developers are members of the Internet Payments Panel, an initiative of Australian Commonwealth Government's "Business Entry Point". The Panel is made up of members who have been selected on the basis of published criteria and who meet stringent government requirements. The goals of SET, as outlined in its Business Plan, were used as a basis for the open-ended questions, which were sent to the member of the Panel via e-mail. Telephonic interviews were conducted with product managers and technical experts of payment vendors actively involved in developing payment products for the local and global markets. Product details were obtained from the technical information documentation provided by the vendors.

9. Discussion of the Results

Of the local Internet payment providers analyzed more than 70% had not implemented SET in their products or had no intention of doing so in the near future.

The preliminary results reveal that the recurrent theme amongst those payment product vendors that did not implement SET in their solutions was the cost of implementation and complexity of SET. SET was regarded as an expensive infrastructure, requiring the co-ordination (and trust) of several companies working together. SSL, it was contended, was far quicker and simpler to install.

The need for rapid deployment of e-Commerce services and functions was one of the higher priorities for companies in this business (next to cost), and the complicated technological architecture of SET with its associated rules, standards and regulations was seen as slowing this process. Although SET had global backing, some saw it as having "promised much but delivered very little to date". Until widespread fraud or regulation mandated SET implementation, there was little incentive to make the investment in time and money.

SET was also criticized for its limited functionality, with one respondent making the point that the credit card number was not the only important information in a transaction, and that SET only addressed this one issue. On the issue of obtaining critical mass, Internet payment product developers have found no real demand for SET from the merchants themselves.

The other comments from the respondents in regard to the reasons for the slow uptake of SET are summarized in Table 1.

On the issue of infrastructural deficiencies that developers saw as inhibiting the more widespread deployment of SET in local Internet payment systems, the general response was that many of the major financial institutions themselves had not made provision for SET. There was no clear commitment by the banks to adopt the standard, which would, in turn, have generated the need to adopt the standard. As a result very little in the way of software development tools, test environments and technical support was forthcoming from these institutions.

To comply with the SET standards and to be "SET MARKED" required a lengthy certification process that all products, solutions and components had to pass. This was a cost to be borne by the developer. Several of the software vendors building SET applications as yet did not have SET-compliance seals of approval on their products. Criticism has also been leveled at SET's perceived slow performance.

On the other hand the protagonists for the SET protocol argued that SET, rather than being competitive in function, was the next logical evolutionary step from SSL. As SSL was not designed to authenticate all the parties concerned in a transaction – its value to combat fraud, as Internet trade volumes grew and security concerns escalated, was limited. Migrating from SSL to SET becomes a necessary evolution as organisations' business cases demonstrate the need for secure e-Commerce.

One expert's view was that, with technology having evolved at the rate it has, there were no real infrastructural deficiencies inhibiting SET adoption at present. SET has seen ongoing development since its initial beta release in 1996, and that a large part of this development had focused on the protocol's initial interoperability issues. The majority of these were now resolved.

Installing SET was the same as any other mission-critical systems – it would involve "up-front investment for long-term reward". The road to secure electronic commerce did have cost implications for Internet retailers no matter whether they chose to implement SSL or SET as their transaction protocol. Using SET merchants would re-coup their investments and actually save money by combating Internet

fraud. As well as eliminating the need to pay out for charge backs, merchants who choose SET will actually win over more customers by protecting them from Internet fraud and privacy infringements.

Certain developments might also boost SET adoption. Card issuers have lowered the fees SET merchants pay to process purchases. They have also removed chargeback requirements that make merchants responsible for proving that a particular transaction took place. Another argument put forward was that any other infrastructure that could potentially emerge would, in order to succeed, need the same level of financial commitment by the major-credit card companies that SET already has. Banks, vendors, and analysts say that future version of SET will bear little resemblance to today's Version 1.0.

On the question of the adequacy of SSL another problem with the protocol was raised. SSL encrypted the whole web page, including all of the complex graphics. To overcome this, minimal graphics is usually used on SSL protected pages in order to reduce the impact on performance, but this was being done at the expense of consumer appeal. Within SET, only the sensitive information in the transaction is encrypted.

As regards statements such as "SET is slow" the argument is said to lose its relevance because with cryptographic hardware accelerators either SET or SSL can easily be fast enough. Any very minor difference between the investment required in a server that supports SET and one that supports SSL is outweighed by the additional security and trust benefits from SET. The Garner Group's comparative analysis on SET and SSL performance also confirmed this by putting both through tests on different loads[22].

Issues	**Typical responses**
Reasons for slow uptake	• Cost of implementation • Better alternatives • Co-ordination difficulties with parties concerned • Promised much and delivered little • Limited use • No demand • Lack of marketing & technical expertise • Limited benefits • Different consumer certificate for each credit card brand required
Infrastructural Deficiencies in SET	• Complexity • Cost of implementation • Certification process lengthy and costly • Limited acceptance from major financial institutions • Lack of software development tools • Lack of test environments • Lack of technical support from financial institutions

Table 1: *Barriers to SET adoption: System Developers Responses*

The common denominator among all the current payment systems analyzed is that they attempt to guarantee the security of transactions by applying various technologies to the transmission of the financial information. Table 2 lists the security mechanisms being currently employed in non-SET compliant products.

Service Definitions	**Technical Features and Design Solutions**
Confidentiality of payment information	• 128 bit encryption • 1024 bit encryption • Payment details stored on secure host • SET wallet • Partial credit card numbers stored
Confidentiality of order (merchandise) information	• 128 bit encryption • Logon & password • ‘ secure tunnel ‘
Data Integrity	• Direct Line to banks • 128 bit encryption • RAID and SMP • 1024 bit encryption
Authentication of payer	• None • Digital Certificates • Registration authority (RA) & SET public key security and certificate management • Proprietary
Authentication of merchant	• None • Secret key • Digital Certificates • Registration authority (RA) & SET public key security and certificate management
Security and system design best practice	• Bank Audit • AS2805 compliance • High performance security engine • Modular architecture • Internal system checks and balances through back-office integration • Use of external parties (Certification Authorities) • Firewalls • Data Protection
Transport protocols	• EFTPOS networks • Open systems and TCP/IP • API support for new protocols • SNA
Hardware and Software Interoperability	• Windows NT, HP, Solaris, OS390, MAC, Unix • Java based • Web browsers • IVR • API support • CORBA, EJB

Table 2: *Service Definitions: Technical Features and Design solutions*

Several products only supported a rudimentary authentication process. All of the products analyzed used a minimum 128-bit level of encryption to ensure data integrity. Some offered as high as RSA 2048 bits. To further ensure integrity, secure tunnels and direct lines are provided for the transmission of information via the PC.

10. Future Work

The response from this exploratory study has revealed a great divide between the protagonists and the antagonists on the role of SET.

Having established a preliminary set of the major security issues confronting payment system developers today, this study can provide the starting point for a Delphi type investigation in which these issues can be systematically identified and consensus reached amongst the experts in the field.

Several of the problems with SET that were raised were more a perception of the problem that the actual reality of the situation. For example, conducting experimental studies and developing cost-benefit analyses of the competing systems could possibly argue against the concerns of cost and complexity that vendors have associated with SET implementations - issues that were raised several times in the interviews.

These analyses, combined with further intended interviews with respondents, and case studies of individual payment product vendors, are expected to yield valuable insights into questions related to building a more secure payment infrastructure (with or without SET). Further research in this area will be of benefit to all of the stakeholders concerned, namely, consumers, financial institutions, merchants, payment system developers, regulators and certification authorities, and also the IS community at large.

11. Limitations

Some of the payment products have been developed overseas and adapted for use locally. The technologies adopted and consequently, the views expressed by the respondents, might well have been influenced by attitudes of their overseas parent companies. This study also relies on individual perceptions of the problems, and the element of bias arising out of vested interest cannot be discounted. The use of alternate methods of data collection in future studies would increase the validity of the findings.

12. Conclusion

To achieve greater acceptance, the payment systems will need to provide for, to a lesser or greater extent, confidential transmission of information, authentication of parties involved and integrity of payment instructions. From the analysis of this

initial study it is evident that security is being seen as a trade-off between what is acceptable and what is affordable. Any security solution should strive to be as transparent as possible so that users will not resist its implementation. This seems to be the attitude adopted in the design of many of the payment systems that were studied. But standardization of payment infrastructure – not of payment products – is required.

Although SET as a "would-be standard" is not in widespread use right now – some say because of its complexity and costs, others say that infrastructure building takes time and that it is too early to judge – it is at least a paradigm for secure payments over the Internet. Even if SET does not become the future de-facto standard, it will be the point of reference for further standardization of this kind. On the other hand, while SSL might have its limits and is not seen as safe as SET, it is still seen, in the short term at least, as being adequate for the purpose by several of the payment vendors.

References

[1] Anthouse Interactive. The SET Business Case [Web Page]. 28 September 1999; Accessed 28/01/2001. Available at: www.anthouse.com.

[2] Asokan, N; Janson, Phil; Steiner Michael, and Waidner, Michael (IBM Research Divison). The State of the Art in Electronic Payment Systems. Computing Practices IEEE. September 1997; 28-35; ISSN: 0018-9162.

[3] Baltimore Technologies. Secure Internet Banking [Web Page]. Accessed 01/11/2001. Available at: http://www.baltimore.com/library/whitepapers/mm_internet_banking_security.html.

[4] Bohle, Knud; Rader, Michael, and Riehm, Ulrich. Editors. Electronic Payment Systems in European Countries: Country Synthesis Report. Final ed.; European Science and Technology Observatory; 1999.

[5] Brockhoff, Anne. Number of online shoppers rises, but they harbour fears. Kansas City Business Journal. 06 May 1998; 16(38):23; ISSN: 0734-2748.

[6] Business Wire (DV). New Electronic Commerce Survey Finds Internet Poised to Become Nation's Cash Register. Business Wire. 22 June 1998.

[7] Committee on Payment & Settlement Systems. Core Principles for Systemically Important Payment Systems: Part 1. Basel, Switzerland: Bank of International Settlements; July 2000.

[8] Dahlstrom, Erik, The Institute for Prospective Technological Studies (IPTS). The common future of wallets and ATMs? Mobile phones! Electronic Payment Systems Observatory - Newsletter Nr. 2. October 2000; [1&2].

[9] Han, Helen. Cantech Secures Shoppers' Trust. The Austrlian Industry Standard. 06 January 2000.

[10] Jayawardhena, Chanaka and Foley, Paul. Overcoming Constraints on Electronic Commerce - Internet Payment Systems. Journal of General Management. Winter 1998; 24(2):19-35.

[11] Larry, Loeb. Secure Electronic Transactions : introduction and technical reference. USA: Artech House; 1998. ISBN: 0890069921.

[12] McAndrews, James, Senior Economist and Research Advisor (Philiadelphia Federal Reserve Bank - Research Department). How will we pay on the Internet? Consumers' Research Magazine. April 1997; 80(4):29; ISSN: 97043020049.

[13] Moodie, David. e-Commerce on 'exponential curve'. The Age. 06 January 2000.

[14] OECD Council. Guidelines for Consumer Protection in the Context of Electronic Commerce [Web Page]. 12 September 1999; Accessed 29/11/2000. Available at: http://www.oecd.org/dsti/sti/it/consumer/prod/guidelines.htm.

[15] Petersen, C, (ed.). Secure Electronic MarketPlace for Europe. SEMPER Consortium; 31 August 1996((AC026/SMP/CT2/DS/C/005/b1)).

[16] Rodgers, John, Special Advisor on Information Security. The Security of Electronic Payments Systems [Web Page]. 15 June 1999; Accessed 01/10/2001. Available at: http://www.dsd.gov.au/infosec/publications/securing-payments.html.

[17] SEMPER (SEMPER Consortium). New Payment Instruments Prototype10 December 1997.

[18] SETCo. SET Secure Electronic Transaction Specification Book 2: Programmer's Guide Version 1.0 [Web Page]. 31 May 1997; Accessed 28/01/2001. Available at: www.setco.org.

[19] SETCo. What is SET [Web Page]. 2000; Accessed 17/01/2001. Available at: http://www.setco.org/certificates.html.

[20] SETCo. SetCo Backgrounder [Web Page]. March 2000; Accessed 17/01/2001. Available at: www.setco.org.

[21] Time. The Internet Economy. Time. 20 July 1998: 19.

[22] Tocq, Chris Le and Young, Steve. SET Comparative Performance Analysis. Garner Consulting; 11 February 1998.

[23] VeriSign. NetSure Protection Plan Summary Version 2.0 [Web Page]. 06 October 2000; Accessed 25/01/2001. Available at: https://www.verisign.com/repository/netsure/summary.html.

[24] Zaba, Stefek. Tools and Protocols for E-Commerce. Elsevier Advanced Technology; 1999 (Information Security Technical Report; 3 (2)).