TRENDS IN ELECTRONIC COMMERCE SECURITY: A MANAGERIAL BRIEF AND TEACHING NOTE

Ajit Kambil
Assistant Professor
Department of Information Systems
Leonard N. Stern School of Business
New York University
44 West 4th Street, Suite 9-82
New York, NY 10012-1126
(212) 998-0843
fax: (212) 995-4228
akambil@stern.nyu.edu

Working Paper Series
Stern #IS-96-25

Trends in Electronic Commerce Security

The Internet and similar networks provide new infrastructures for communications and commerce. These open networks interconnect computers across many different organizations with dramatically lower communications and distributed applications development costs. This motivates businesses to transfer commercial activity from closed private networks to open networks like the Internet.

However, open network architectures are vulnerable to a number of different security threats. While many different hardware and software solutions exist to secure transactions over the Internet, greater consensus is required by companies and consumers on the processes, organizations and application of existing technical solutions for secure electronic commerce. Greater consensus on security among trading parties will lower the costs of electronic commerce and accelerate its deployment on the Internet.

1.0 Trends in Electronic Commerce Security

Widespread electronic commerce over the Internet will have a dramatic impact on the organization and execution of financial and non-financial transactions. As discussed in our previous report, electronic transactions promise to reduce transaction costs substantially. This will alter industry structure and competition by increasing price competition and reducing the margins of firms that cannot execute transactions in an efficient manner. Many large vendors (Microsoft, IBM, AT&T, MCI, EDS) now embrace the Internet as the infrastructure to support electronic commerce applications. However, the consumer's and business's trust in the security of the Internet will be a key factor in the rate of adoption and electronic commerce over the Internet.

The Internet is inherently insecure for transactions as it can be compromised at several points, including the user's computer, the merchant's or service provider's system or at any intermediate point between them on the network. This is because the Internet consists of many different computer networks that are all interconnected using a common protocol. Due to this open network architecture, messages traverse many different networks between source and destination. For example, when a user transmits a credit card number over the Internet to a merchant, this number passes through several computer systems, including systems of other network users before reaching the merchant's computer. The integrity of the message could be compromised at any of the intermediate points. Furthermore, as business on the Internet grows, it will become more difficult for both the buyer and the merchant to know whether each is legitimate.

A number of methods are available to secure transactions on the Internet. This report identifies the requirements for secure electronic commerce and the major technical solutions available for securing transactions on the Internet. We propose that the technical schemes to secure transactions are well known and widely available. However, companies and industry groups lack any consensus on how to best implement security measures. As these measures are widely adopted, more business-to- business and consumer-to-business transactions will be carried out over the Internet. A variety of different payment and settlement schemes will evolve to support these transactions. These methods will vary in supporting features such as anonymity and transaction costs, for different types of transactions. Eventually consumer transactions will most likely be supported by smart cards due to their superior security and information storage features.

2.0 Creating Trust: Requirements for Secure Electronic Commerce

All traditional commercial activities use procedures or occur within contexts designed to generate trust between individuals or between businesses. These trust mechanisms reduce the commercial risks faced by traders and rely on a variety of factors from prior track records, reputations, and the legal context for an exchange. However, unlike discrete face-to-face transactions where some good is exchanged for cash, electronic commerce creates both opportunities and difficulties for potential traders. Specifically, it opens the opportunity to expand trade at lower costs over a wider marketplace distributed over a larger geographic scope. Indeed leveraging these new opportunities over an inexpensive global communications infrastructure will be one of the key benefits of electronic commerce.

Open networks like the Internet pose the new requirement of generating trust in an electronic environment. The essential requirements for carrying out secure electronic commerce based on models of traditional commerce model include the need for the following:

- Server security
- Message Privacy
- Message Integrity
- Authentication
- Authorization
- Audit Mechanisms and Non-Repudiation
- Payments and Settlements.

Each of these requirements is defined and discussed below:

2.1 Server Security: Viruses, Trojan Horses and Hackers

Internet commerce requires secure server computers, computers that serve documents, files or programs to users. Server computers with critical applications should not be vulnerable to attack from software viruses or Trojan horses (viruses that are hidden program or documents to be activated at a later time), and unauthorized access over the network from hackers. The primary means to accomplish this is through firewalls and proxy machines that intermediate the relationship between a company's internal networks and the external Internet. Proxy and firewall servers intermediate all Internet communications between a firm and its external environment. Every packet and or file transferred to or from the Internet to a firm's internal machine goes through the proxy or firewall server where it is checked to ensure there are no known viruses or other problems. Such firewall or proxy server software is widely available from many companies although not all organizations adopt this level of security.

2.2 Message Privacy

Message privacy is a key requirement for electronic commerce. Message privacy assures that communications between trading parties are not revealed to others as the message traverses an open network.

2.3 Message Integrity

Message integrity is another key requirement for electronic commerce. It is important that the communications between trading parties are not altered as they traverse an open network.

2.4 Authentication

Authentication procedures generate trust by ensuring that the counterpart to an electronic transaction (who may be located elsewhere) is the person he or she claims to be online. As it is easy to "spoof" machine addresses or electronic mail addresses, methods of authentication are vital for secure transactions and their enforcement.

2.5 Authorization

Authorization ensures that a party to an electronic transaction has the authority to make a transaction, or is authorized to access specific information or computer resources. Authorization is important in managing the risk that employees or others do not make transactions that create economic damage or access key information or computational resources of the organization.

2.6 Audit Mechanisms and Non repudiation

Like normal commercial transactions, audit mechanisms for electronic commerce enable the exchange parties to maintain and revisit a history or the sequence of events during a prior transaction. In electronic commerce, these audit trails could include time stamps or records by different computers at different stages of a transaction. In addition, there need to be confirmations and acknowledgments by the various transacting parties that they have accurately received various messages, and made specific commitments. Parties should not be able to repudiate their prior commitments.

2.7 Payments and Settlements

Electronic payment and settlements systems lower transaction costs for trading parties. Secure payment and settlement systems, that also ensure that the commitments to pay for a good or service over electronic media are met. They are vital for widespread electronic commerce.

There are a number of ways to meet the above requirements for secure electronic commerce. Other than server security, all the different mechanisms rely on some form of encryption. Below we outline the basics of encryption and discuss the different ways in which firms can apply available encryption techniques to meet the requirements to secure transactions over the Internet.

3.0 Securing Internet Commerce

3.1 Encryption

Encryption of communications has traditionally been used to ensure the confidentiality of information. In electronic communications, encryption is the transformation of electronic information based on a secret key code. This transformation makes it difficult for unauthorized users to access or review the information.

There are two basic forms of encryption, **symmetric** and **asymmetric**. The DES, or Data Encryption Standard, is a United States' Government standard for symmetric encryption of large blocks of data. This scheme encrypts or transforms the data being sent over a network using a secret encryption key in such a way that the message can be decrypted at the other end only by using the **same** secret key used initially to encode the message. Symmetric cryptography is difficult to break computationally. However, it is unsuitable for use by itself for encrypting transactions in the Internet. This is because both the sender and receiver must have knowledge of the same secret encryption key. For efficient electronic commerce, this would require transmission of the secret key over the open Internet network. As the transmission of keys can be intercepted, symmetric key encryption cannot be used by itself. Symmetric key encryption is also difficult to scale up to a large number of users. Each user would need to maintain a different key for every other user or merchant with whom they transact or exchange messages.

Asymmetric cryptography, also referred to as public key cryptography, addresses the major limitations of the symmetric cryptographic schemes. It permits does not require the secure initial transmission of a code key (which is the case for symmetric cryptography) and it is scalable to a large number of users. Thus, it is well suited for use over the

Internet. For example, in the RSA[1] public key cryptography scheme, the encryption and decryption of data are performed using key pairs. Both the sender and receiver of a message each own a unique key pair. One key within the pair is called the *public key*. This public key is published widely. The other key in the key pair is called the *private key* and it is kept private to the party owning the key pair. The private key is never transmitted over the network.

To send a secure and signed message from a sender to receiver, the sender encrypts the message using the receiver's *public key* and digitally signs the message using his/her (sender's) *private key*. On the other end of the communication the receiver decrypts the message using his/her *private key* and verifies the digital signature by using the sender's *public key*. This example illustrates a powerful property of the RSA asymmetric key encryption. Given a key pair, if the message is encrypted by it public key, it can be decrypted by the corresponding private key in the key pair and vice versa. By taking advantage of this property, communicating parties only have to reveal their public keys to enable secure encrypted communications as illustrated in the example above.

The advantage of asymmetric cryptography is that secrecy is not needed for the public key. This means that only a single key pair needs to generated for each user or service provider. It also simplifies the distribution and management of the keys. The disadvantage of using this scheme over symmetric cryptography is its computational requirements and speed of decrypting messages. Asymmetric key encryption and decryption require more computational power and hence the performance of these systems are much slower than their symmetric counterparts.

Thus, asymmetric cryptography is rarely used in isolation due to the performance issues. Instead it is used in combination with symmetric schemes. This kind of hybrid implementation is seen in several commercial Internet applications. Asymmetric cryptography is used to encrypt a symmetric encryption key and a checksum[2] which is then shared securely between a sender and receiver. Next the sender and receiver use the symmetric encryption key and checksum to encrypt and protect the actual message that is transmitted. This technique is popular in systems used to protect electronic mail,

[1] RSA is a public key cryptography system developed by Rivest, Shamir and Adelman (hence RSA) in 1977. This is a patented system that held up well against various techniques to break the system.

[2] A checksum is a number generated at the time the message is sent which describes various properties of the message, such as the number of characters or specific types of characters in a message. It is used by the receiver to ensure that the message was not altered during transmission.

including Privacy Enhanced Mail(PEM), and Pretty Good Privacy (PGP) and in secure versions of protocols for the World Wide Web including the Secure HTTP (SHTTP) and the Secure Sockets Layer (SSL) protocols.

The application of the above encryption techniques to solving different security problems is discussed in the next section. Today, Public Key Partners a Sunnyvale, California company owns the key patents to the RSA asymmetric key technologies. Software and technologies incorporating this de facto standard are distributed worldwide by RSA Security Inc., which provides licenses and key software to generate keys and to decode and encode messages to other vendors.

3.2 Trends in Internet Security Protocols for Privacy and Message Integrity

In a distributed communications system such as the Internet, developers of applications can choose to implement security protocols at many different levels within the seven layer Open Systems Interconnect reference model for distributed communications architectures. This model is illustrated below for reference:

Figure 1: The OSI-Reference and TCP/IP Models

	OSI Reference Layer	**Layer Definition**	**TCP/IP**
7	Application	Specifies distributed client-server applications	Applications: WWW browsers http, telnet, file transfer protocol
6	Presentation	Specifies protocols for translating data format	
5	Session	Specifies protocols for starting and ending a communications session across a network	
4	Transport	Specifies protocols for end to end error control	Transmission Control Protocol
3	Network	Specifies protocols for routing messages: such as addressing, and paths for transferring messages on a network	Internet Protocol
2	Data	Specifies protocols for point to point transmission and error control	Data Link

1	Physical	Specifies protocols for transmission of data over physical media	Physical

In any distributed communications applications, each of the protocol levels below the applications level are applied to the data in order for it to be formatted, transmitted, and recovered after transmission across the network.

Three particular levels at which secure protocols exist, or are being developed and implemented, are the applications, session and network levels. Using security protocols at each of these different levels imposes different costs on developers of applications that run on the Internet.

Network Level Security: Network level security is important because as packets of data traverse the network, their source and destination addresses are accessible to all intermediate network nodes or routers. Proposals for IPnG (the next generation of the Internet addressing scheme) will implement the encryption of key elements of packet header information to ensure that the privacy of key address information is maintained. In addition, these changes will reduce the likelihood of the success of "spoofing" or making a specific computer on the network appear as if it were another. IPnG will require a substantial upgrade in the software and capabilities of routers that currently switch traffic over the Internet. These changes do not protect the message. But they provide additional security for information about the source and destination of the message.

Session Layer Security: Secure Sockets Layer (SSL), a protocol devised by Netscape Communications, integrates security services at the session layer for applications that use a socket (TCP style) transport interface. SSL is designed to fit between application protocols, such as the hypertext transfer protocol (WWW service), file transfer protocol and telnet protocols and transport layer protocols such as TCP. It provides an encrypted and integrity-protected layer over which higher level protocols may be transmitted. SSL's role in a client-server connection is to encrypt outbound and decrypt inbound packets of a protocol specific datastream. Encryption keys are randomly generated during the session. For U.S. users, key sizes will be upto 128 bits long; and non-U.S users will have keys sizes of 40 bits. The larger the key size the more difficult it is to compromise the security of the encryption.

The advantage of SSL is that application developers on the World Wide Web (WWW) do not have to worry about writing code to ensure message integrity and privacy of information transferred between users using client-server applications adopting SSL. Thus web developers can develop applications without worrying about the details of encryption. If, for example, a form is implemented on WWW page to accept credit card numbers, users can be assured that the credit card number will not be decrypted while the information is traversing the Internet. It is important to note that SSL does not protect the integrity of the documents which are stored on a server. This would still require server security such as firewalls. To ensure documents stored on servers are not changed they should be digitally signed by the author. SSL also does not provide authentication of sites, or electronic counter parties.

Applications Layer Implementations:

Applications layer implementation of security implements encryption within a specialized software application or in separate applications dedicated to security. A number of tools exist to provide encryption to insure message privacy and integrity. These include:

•Pretty Good Privacy (PGP), is a scheme devised by Philip Zimmerman, that creates a random session key for a message, and uses the relatively inexpensive IDEA algorithm (symmetric cryptography) to encrypt the message. The RSA algorithm (asymmetric cryptography) is used to encrypt the session key with recipient's public key to exchange the session key securely over an open network. Then the encrypted message and the encrypted session key are then bundled together for transmission. This is an inexpensive and popular way of encrypting electronic mail.

• Privacy Enhanced Mail (RIPEM) is a scheme devised by Mark Riordian to sign documents or data, and to encrypt and decrypt them. It uses RSA algorithms and is supported by popular mail packages -- for example Gnu Emacs and ELM. RIPEM creates a digital signature on the document that is based on the message as well as private key of the sender. The public key of the sender can then be used to authenticate the originator of a message and the digital signature can be used to verify the message has not been tampered with during transit. Thus, RIPEM can ensure message integrity as well as privacy. If the privacy of the message is less important, only the signature is sent as an encrypted message.

•Secure HTTPD is a security protocol supported by a consortium of NCSA, EIT and RSA labs. In this implementation, security for transactions on the Web is provided at the application layer. SHTTPD allows a web browser to request a digital signature for a retrieved document. The digital signature is a checksum of the document encrypted using the private key of the document's author. The checksum can be decrypted with the public key of the author and the integrity of the document verified. Links to documents under SHTTPD identify the author of the document whose public key must be used to verify the signature.

Similar to SSL, the SHTTPD scheme allows protected transmission of data in WWW forms sent by the user to the server. This is accomplished by encrypting the data stream using a code key that is sent to the HTTP Web Server, using HTTP server's public key to encrypt the code key during transmission. The primary use of this feature is to allow users to safely provide servers with passwords or credit card numbers.

•Applications specific implementations of security: A number of companies are developing specialized applications that leverage the Internet's low cost infrastructure for communications. For example, Premenos is a leading supplier of Electronic Data Interchange software for business to business communications. Premenos's TEMPLAR product line implements RSA based encryption of EDI messages in its own software so that it does not have to rely on encryption provided by other vendors at lower layers of the seven layer reference model. Depending on the security requirements of specific contexts, more specialized applications are likely to implement security at the applications layer. In addition to ensuring message privacy and integrity, specialized applications at this layer will also support authentication, authorization and other desired feature for electronic commerce discussed in the next section.

Due to computational requirements, asymmetric cryptography is not typically used to encrypt messages in transaction processing applications. The asymmetric cryptography algorithms are not efficient at handling many thousands of operations per second on behalf on different clients. The scheme is best for store and forward applications like electronic mail and WWW document transfer.

Given the dominance of Netscape in browser markets SSL is likely to become a key standard, but developers will complement the capabilities of SSL with higher level security implemented at the application layer. IPnG is unlikely to be widely implemented in the next two years.

3.3 Authentication and Authorization of Electronic Counter Parties on the Internet

While cryptography can assure message integrity and privacy, it does not by itself assure that an electronic counterpart to a trade is authentic or authorized to make the trade. Given that asymmetric cryptography is the most appropriate for open networks, transacting parties must know the other party's public key or rely on a trusted third party to certify the other user's public key is valid. Without a trusted third party, it is possible for an attacker to replace the public key of a participant with a different key (for which the corresponding private key is known by the attacker). This allows the attacker to decrypt messages using the fake key and generate messages signed by the fake public-private key pair.

Similarly, when using purely symmetric cryptography, a trusted third party intermediary with whom both parties share an encryption key can generate and distribute a new key, called a session key, to be used between parties that do not share a key directly. The use of such third parties for the exchange and certification of encryption keys is closely tied to authentication which binds the encryption keys to specific individuals, groups or organizations.

Authentication and authorization of end users is enabled by two main mechanisms in a distributed computing environment. These include: the use of certificate authorities to bind specific parties to public key, and the use of Kerberos type systems to authenticate user access to the computing environment. In addition, application-specific and smart card solutions are also feasible. These are discussed below:

Certificate Authorities and Hierarchies:

Certificate authorities (CA) provide a mechanism to bind a public key to an individual, group or organization. This is critical in implementing an authentication or authorization system. The following steps illustrate how a certification authority works to authenticate an end user.

i) The CA will widely publish its public key so that its available to all users.
ii) The CA, as a trusted third party, will verify that a specific person, or institution is bound to a specific public key. The public keys of different persons or institutions will be stored by the CA on a secure computer system. The verification of the identity of a user can depend on traditional paper documents or other direct authentication mechanisms.
iii) If two parties now want to trade electronically, they can send a request to the CA for the other party's public key. This request can be sent using the CA's widely published public key to encrypt the request. As the CA holds its private key, it can review the request. The request can also include the requester's public key.
iv) The CA can then send the public key of the counterparty to the requester. This message is encrypted by both the CA's private key and the requester's public key.
v) The requester then decrypts the message from the CA, using his private key to ensure the message was not tampered with in transit.
vi) The requester then decrypts the message further, using the CA's public key to verify that the message came from the CA. This reveals the true public key of the counterparty.
vii) As the counterparty was previously authenticated by the CA, the requester of the public key can be assured that this is the true public key of the counterparty and that the counterparty is authentic.

Once a certificate authority is established, a certificate hierarchy can be implemented to further verify users, as well as provide a degree of authorization for transactions. Certificate hierarchies (CH) establish a "chain of trust".

Consider a the authentication requirements for a trade say of foreign exchange executed by traders in two different banks, A and B, over an open network. First, each trader needs to verify that the other is a legitimate employee of their respective banks. Second, it's important to verify that both employees have the authority to trade these specific monetary instruments. An industry level certificate authority is unlikely to track the verify the public keys of individual employees. It can, at best, verify the public keys of the firm in which the employee works. Given the firm level of certification, the firm can then certify the forex (foreign exchange trading) group's public key within the firm, and the employee's public key within the firm if the employee is valid. This can be used by the counterparty to decrypt, verify and authenticate the messages from both the employee and the forex group.

In the trade, the employee of the counterparty is verified by checking his signature using the employee's public key. This public key was previously verified by the firm level certificate. The authority to trade is verified by using the forex group's public key to check the message that the employee is authorized to make the forex trade. This chain of certificates required to authenticate the trade is known as a certificate hierarchy.

Distributed authorization services are critical for widespread electronic commerce. Without the distributed authorization service implemented by a CA and CH each party would have to maintain its own list of counterparts it could trade with and their public keys at any point of time. The certificate authority approach to distributed authorization enables parties to provide information such as group membership, or authority to perform a specific operation. Upon receiving such a certificate, a user can verify the signature of the authorization server, and check to make sure the rights conveyed by the certificate allow the operation requested by the other users.

A number of parties provide certificate authority services. RSA Security's new subsidiary Verisign is a leading provider of the technologies for certificate authorities as well as a CA service. The U.S. Postal Service also provides a certificate authority service. This service is widely seen as a service that can certify consumers, and verify postal addresses for delivery of consumer goods. However, the Postal Service CA is inadequate for specific industry needs. For example, securities trading will require a high degree of security as well as verification of trading parties. A higher level of trust is probably best generated by a trade association certifying member organizations to the required standards of the industry rather than a more generic certification at the level of the Post Office.

While the technology for certification authorities is widely available, their widespread adoption is hampered by the lack of organizational and legal consensus in different industries on how to implement policies for certification and any attendant legal liability. Various industry trade groups in the United States are investigating ways of implementing CA to meet the needs of their industry. The secure implementation of the signed authorization certificates depends on the integrity and the authentication services. Thus, organizations will have to build substantial safeguards to assure the CA system is not compromised.

Kerberos

Authorization is required to establish what services on a host system, a remote user can access. For example, a salesperson needs to access his company's host computer over the Internet. How can this be done in a secure manner?

The Kerberos system is an authentication protocol that can be embedded in any network protocol to identify the user making a request accurately. On the Internet, password based authentication is not suitable, as these passwords can be intercepted when they are sent across networks. An authentication protocol is required to prove the user has knowledge of the correct password without actually sending the password across the network. This can be accomplished by using an encryption key in place of a password and proving the knowledge of the encryption key.

The Kerberos authentication protocol, developed at MIT in 1985, is based on symmetric cryptography. In this implementation, when the salesperson wishes to communicate with his company's host on the Internet, the Kerberos authentication server is contacted by sending the username, the server name and any additional information. Next, the Kerberos server randomly generates a session key and returns it to the requesting user, encrypting the key in some information derived from the user's password which was previously registered in advance with the host server. This encrypted session key is returned together with a *ticket* encrypted by the server that contains the name of the user and the session key.

The encrypted session key and the ticket received from the Kerberos server is cached by the user system, reducing the number of requests to the server. To prove the authenticity to the host, the salesperson enters his password to decrypt the session key. This password verification is now totally local to the client (salesperson's machine) side. Next, he or she forwards the *ticket* along with a timestamp encrypted in the session key from the ticket. The host system decrypts the ticket and uses the session key within it to decrypt the timestamp. If the timestamp is recent, the server knows that the message was sent by someone who knew the session key. Since the session key was only issued to the user named in the ticket, this authenticates the client. If the client requires authentication from the server, the server extracts the timestamp, re-encrypts it using the session key and returns it to the client.

Thus, the Kerberos server acts as a trusted intermediary in the authentication process. Both the users, merchants or service providers using Kerberos have to register their encryption keys (passwords) in advance with the Kerberos server itself, and not with each party with which they will communicate. The issue of securing this server against attackers becomes important. The server generates a session key when needed and distributes it to the client, and places it in the ticket where it can be later recovered by the merchant or service provider. This session key can then be used directly by the client and the service provider for encrypted communication as described earlier.

Application Specific Authorizations

Besides the use of a certificate authority, firms may use proprietary applications which have various specialized levels of built in authorization capabilities. These are likely to be adopted by financial services firms for specialized transactions.

Smart Cards

Smart cards permit hardware-based authentication and encryption independent of the network or the computer device to which the card reader is attached. Smart cards can have both memory and a simple processor embedded in them. If a user wants to connect to the network and be authorized to access resources over the network, he or she could insert the card in the card reader (such as a PCMCIA) slot and enter a password. The card would interpret and authorize the user's password much like how PIN codes work for credit cards. However, in addition to authenticating the user, the cards contain the user's encryption keys. Thus, the card can sign messages on behalf of the user without divulging the keys to the computer device to which it is connected.

This network and device independence make smart cards very attractive for authenticating parties in electronic transactions. Today smart card readers remain about $200 making it expensive to use these devices widely. However as prices fall and the functionality of cards increases for other purposes, smart cards promise to be a preferred choice for authenticating users of electronic commerce.

3.4 Establishing Audit Trails, and Non Repudiation

Besides message integrity, privacy, user authentication, and user authorization, secure electronic commerce requirements include the ability to audit transactions, and non-repudiation of commitments, payments or settlements.

As illustrated by the notion of a certificate authority and hierarchy, audit trails can be established by the certificates applied to messages during various stages of a transaction and the verification of digital signatures. Other key features that can be provided by third parties to transactions include timestamps and records of inter-organizational transactions for dispute resolution. Again, the standards for these audit mechanisms are most likely to evolve to meet the requirements of specific industries.

True non-repudiation of messages, in terms of the origin and receipt and acknowledgement of messages, is also important for electronic commerce. This means a party to a transaction cannot deny he or she received a particular message or payment after the fact.

The encryption and the digital signature mechanisms discussed previously can be used to send acknowledgments of data receipt and confirm data origination. These techniques are most likely to be built into specific applications for electronic commerce.

3.5 Secure Payments and Settlement Systems

Secure payment systems can be built on the techniques discussed in the prior sections of this report. A number of different products have been developed or are in development for secure payment over electronic networks. However, no dominant standard has yet been established for consumer or business to business payments. Secure payment systems can be broadly classified into three categories:

- •electronic cash systems
- • electronic check systems
- •card based systems

Electronic Cash Systems

Cash consists of a token that can be authenticated independently of the issuer. Electronic cash consists of electronic currency certificates which customers buy from a currency server, paying for the certificates through an account established with the currency server in advance or through other forms of payment. The merchants on receipt of these electronic certificates can deposit them in their accounts or spend it elsewhere. The principal advantage of electronic currency is its potential for anonymity. However, on the other end, there is a need to maintain audit trails to prevent double spending. Examples of the electronic cash models include: Digicash, NetCash, and Mondex.

Electronic Check Systems

These systems are also referred to as debit-credit systems. Checks are payment instruments whose validity requires reference to the issuer. Electronic versions of this model include First Virtual's current products. Other products in development include NetCheque, Carnegie Mellon University's NetBill and the Financial Services Technology Consortium's Electronic Check project. In this model customers maintain accounts on a payment server and authorize charges against those accounts. These implementations rely on the authentication and authorization services like those described earlier in this report. Electronic check systems can be designed for micro-payments less than a dollar and implemented at low transaction costs.

Card-Based Systems

Card payment systems use the existing credit or debit card payment infrastructure. Such schemes have many structural similarities to check models except that solutions are constrained by that structure. A key feature of card payment systems is that every transaction carries insurance.

Card systems include offerings by CyberCash, Mastercard, Visa and other firms. Mastercard and Visa will use the secure electronic transactions standard supported by Netscape. In the card systems model, the customer's credit card number is encrypted using asymmetric cryptography so that it can only be read by the merchant, or in some cases a third party payment processing service. This allows existing credit card customers to use the Internet and leverages the existing credit card infrastructure to carry out transactions. Users need not be registered with a third party or a service provider to carry out transactions. This mode of payment is however not suitable for carrying out micro-payments as required for information goods. The transaction costs involved in the clearing credit card payments through the existing financial infrastructure remains high.

The different secure payment systems currently available on the Internet illustrate the feasibility of secure electronic commerce. A variety of different payment and settlement schemes will evolve to support transactions on the Internet. These will vary based on the importance they place on different features such as anonymity, micro-payments, ease of use, transaction costs for different types of transactions. Thus, no one system is likely to be the dominant standard.

4.0 Conclusions

A variety of techniques based on public key encryption support secure transactions over open electronic networks. This discussion addressed the requirements for message privacy, integrity, user authentication, authorization and non-repudiation. It also identified three different types of payment and settlement systems available for electronic commerce.

We expect widespread adoption of the technologies discussed in this report to enhance the use of the Internet for electronic commerce. The critical constraint is not technology as much as consensus on appropriate standards for electronic commerce. Different industries and organizations need to evolve new standards for electronic commerce that best meet the requirements of their industry.