Introduction

Cybertrade, or electronic commerce, has taken place for many years in the form of electronic data interchange (EDI) although this has been restricted to a few sectors of industry such as banking, insurance, shipping and the motor trade. Where EDI is used it is confined to a closed user group where the parties have probably enjoyed a good working relationship and already trust each other. EDI is usually regulated by the use of an underlying interchange agreement setting out the contractual and commercial obligations between the parties and data transfer will most likely consist of the processing of purchasers orders and invoices and the acknowledgements of orders. In the case of banking, EDI arrangements exist in the form of SWIFT messaging and the CHAPS system and in the case of the insurance sector EDI networks such as LIMNET and the more recently established WIN. All of these types of closed networks still have the potential for fraud and loss but in more open networks where third parties become involved in the transaction then there is a greater need for security in order to avoid fraud, dispute or loss.

Electronic commerce is taking place in an increasing manner via the internet, which is becoming the fastest growing communication channel this century. The exponential growth of the internet is causing businesses to rush into cyberspace because they perceive the net as a Klondike of digital opportunity where riches and opportunities await early web site prospectors. In the foreseeable future, the internet is perceived as the replacement for our traditional method of communication.

There are, however, increasing concerns within the banking, insurance and other financial institutions over the security surrounding electronic commerce, where often the parties have neither dealt with each other before nor is the internet secure for the purposes of confidentiality and message integrity.

The main reason for electronic commerce security is to protect the integrity of an electronic message between the time it leaves the senders application system and the point it arrives on the receiving parties application system. This is known as "end to end security". It should be noted that this only covers the integrity of the message itself and does not deal with the integrity of the respective parties applications systems. Apart from message integrity, security should extend to issues such as:

- The repudiation by one party of receipt or dispatch of a message,
- the risk of hacking or masquerading,
• message modification or tampering, and
• message corruption or loss.

The security of messages and their authentication can be helped by the use of encryption techniques and digital signatures, all part of the science of cryptography.

**Cryptography**

The increasing use of open network communication systems, as opposed to closed networks, poses significant challenges to the implementation of global secure electronic commerce. Among the most significant problem in this area is in relation to information security. The use of the internet for electronic trade poses the challenge of "many to many" transactions.

A secure electronic commerce system requires the implementation of cryptography - the art or science of keeping a message secure. Cryptography can be used to:-

• hide information content:
• establish authenticity
• prevent undetected modification
• prevent repudiation, and
• prevent unauthorised use.

Cryptography can be used to protect the confidentiality of financial data or personal records whether it is in storage or in transit. Cryptography can also be used to verify the integrity of data by revealing whether it has been altered and identifying the person or device that sent it. Encryption techniques are critical to the development and use of national and global information and communication networks and technologies as well as the development of electronic commerce.

**Encryption**

Encryption is the technique by which clear text is scrambled into incomprehensible text and only decipherable by the holder of a secret code key. The method by which electronic messages are scrambled and unscrambled is through a mathematical formula
or algorithm and a number of internationally recognised algorithms are used combining business data with small secret sections of data known as keys. The real value of an encryption system depends upon how difficult it is to unlock without the key and several supposedly secure systems have been cracked. Those that are deemed to be totally secure pose their own security problems for government and security agencies who resent the potential transmission of subversive messages in cyberspace.

Two of the most widely used and accepted algorithms are DES (Data Encryption Standard) and RSA (named after its creators Rivest Shamir and Adelman). DES is a symmetric algorithm in that both parties know the same secret key whereas RSA is an asymmetric algorithm because different keys are required for encryption and decryption. Asymmetric algorithms usually have three code numbers in effect because apart from the private keys of sender and receiver, there is a common modulus and this means it is more secure because even with the possession of the common modulus it is hard to calculate either private key. As a result of the relatively secure encryption techniques that exist today, government agencies wish secret keys to be lodged with trusted third parties.

**Digital Signatures**

As has been stated, public key encryption techniques ensure financial institutions that their messages are secure and that other transacting parties with them are authenticated. Using this technology senders and receivers of electronic messages each possess two keys, one of which is never shared with anybody and the other of which is shared with everyone. These two keys correspond to each other so that whatever is encoded with one key can only be decoded by the other. During the encrypting process the sender of the message encodes the message with the recipient’s public key, making it impossible for any party other than the one holding the private key to decrypt the message. Encryption, therefore, protects the message from all parties other than the recipient without the recipient having to divulge his private key to the sender.

If the process above is reversed then public key cryptography also provides a highly dependable authentication mechanism which has come to be known as a digital signature. A digital signature is an electronic substitute for a manual signature which serves the same functions as a manual signature and more. It is an identifier created by a computer instead of a pen. In technical terms a digital signature is the sequence of bits that is created by running an electronic communication through a one way hash function and then encrypting the resulting message digest with the senders private key.
Digital signature is not a digitised image of a hand-written signature or a typed signature. A digital signature is unique for each document signed because it is derived from the document itself and any change to the document will produce a different digital signature.

A digital signature can serve the same purposes as a hand-written signature in that it may signify authorship, acknowledgement or assent but a digital signature also serves important information security purposes that hand-written signatures cannot.

Assuming an asymmetric system is in place then in order to digitally sign a message the sender will run a computer program that creates a unique message digest or hash of the communication and the program then encrypts the resulting message digest using the sender's private key and the resulting encrypted message digest is the digital signature. The sender then attaches the digital signature to the communication and sends both to the intended recipient.

When the recipient gets the digitally signed communication in encrypted form the recipient's computer runs a program containing the same cryptographic algorithm and hash function that the sender used to create the digital signature and the program automatically decrypts the digital signature using the sender's public key. Therefore, if the program is able to decrypt the digital signature, the recipient knows that the communication came from the sender since only the sender's public key will decrypt the digital signature encrypted with the sender's private key.

The program then creates a second message digest of the communication and compares the decrypted message digest with the digest the recipient created. If the two message digests match the recipient knows that the communication has not been altered or tampered with thereby verifying the integrity of the message.

Because digital signatures are difficult to forge their use binds the signatory precluding a later repudiation of the document. Digital signature technology also forms the basis for formally legally binding contracts in the course of electronic commerce, since they provide electronically the same forensic effect that a traditional paper document and a hand written signature thereon provides.

**Proposals in Europe and the US for Public Key Infrastructures**

A hand written signature is unique to its creator and may be verified by such signature taking place (physically) before the party relying upon the signature or alternatively in the presence of witnesses, or a notary. In the case of a digital signature, this is merely a large strings of bits and is created in cyberspace and not in the presence of the party.
relying upon it. In an asymmetric crypto system or public key system there is a need to verify that the public key is not compromised.

If public key cryptography is to succeed as a method for secure electronic commerce on a global basis, then there is a need to establish a public key infrastructure (PKI) under which trusted third parties (TTP) or certification authorities (CA) would be established to hold keys in order to provide confirmation that the holder of a public key is who he or she purports to be. Without a TTP certifying that a given individual is in fact the holder of a public key, it is impossible for other transacting parties on the network to know for certain that the holder of the public key is not an impostor.

The nearest existing equivalent to an independent TTP is that of the Notary and whilst in Europe the Notary is a public official appointed by the government (or in the case of the United Kingdom, by the Archbishop of Canterbury on behalf of the Queen) and is a profession with strict rules, ethics and training, in the United States the Notary is a far less regulated and qualified profession. Indeed, almost anyone can be a Notary in the United States provided that they pay an annual fee, do not have previous convictions or bankruptcy proceedings against them, and in any event are only commissioned to practice as a Notary for a limited period of time.

The American Bar Association some two or three years ago, recognised the value in creating a higher level Notary for the purposes of providing the role of TTP in the PKI. The American Bar Association within the last two years has worked closely with the European notaries in order to create a higher level Notary known as a CyberNotary and has published its Digital Signature Guidelines in 1996.

The CyberNotary would perform the role of TTP or CA and would be required to have both legal as well as technical ability in the area of authentication of public keys and the provision of digital certificates.

The European Notaries have maintained for some while that since they are public officials and already have years of experience in the authentication and certification of documents which then have proof of law, they are the logical body to provide the TTP services required as part of the PKI.

Notwithstanding the position of the European notaries a number of governments are now proposing a regulated PKI to provide for licensed TTP's. The United Kingdom Government has recently issued a consultation paper on "The Licensing of TTP's for the Provision of Encryption Services", and the German Government has acknowledged the use of CA's within its draft Digital Signature Bill Ordinance within Article 3 of its draft Information and Communication Services Bill.
The European Commission is actively promoting a number of electronic commerce projects which are all intended to anticipate the creation of an European wide PKI and indeed in European Commission's responses to the OECD's proposed "Guidelines on International Cryptography Policy" (now finalised and published March 1997), the Commission have advocated a European wide TTP system.

In the United States the US administration announced a plan in October 1996 to enable the use of stronger encryption products which envisioned a world-wide PKI using key escrow and key recovery encryption services.

Despite the US administrations previous concerns on the export of strong encryption software as evidenced by the Clipper chip policy, they now are making export and re-export of DES and RSA software available, provided that the countries of receipt are not those on the export ban list such as Cuba, Libya, Iran and Iraq.

In envisaging a world-wide PKI the US administration has recognised the need to use CA’s to provide key escrow and key recovery services so that government official may obtain under proper legal authority and without co-operation or consent of the user plain text or encrypted data and communications and in particular the individuals private key.

Use of Trusted Third Parties for Key Escrow and/or Key Recovery

The US, UK, Germany and European Commission all recognise that PKI will require the establishment of a regulated TTP or CA system.

In the UK Government's Public Consultation paper entitled "Licensing of Trusted Third Parties for the Provision of Encryption Services" a TTP has been described as "an entity trusted by other entities with respect of security related services and activities. A TTP would be used to offer value added services to users wishing to enhance the trust and business confidence in the services they receive and to facilitate secure communications between business trading partners. TTP's should have trust agreements arranged with other TTP's to form a network, thus allowing a user to communicate security with every user of every TTP with whom his TTP has an agreement."

A CA as defined under US State law (Utah State) or a Certification Officer as defined in the draft German Signature Bill is a TTP or entity that ascertains the identity of a person called a subscriber and certifies that the public key of a public private key pair used to create digital signatures, belongs to that person.
There is a difference between the role of the TTP as envisioned by the UK Government's recent paper and the CA as envisioned in the German Draft Signature Bill. The difference lies not in the name of the officer or entity within the PKI but in the particular role that it is performing.

The confusion that presently arises in much draft legislation is that on the one hand governments require legitimate access to encrypted messages and therefore require private keys to be placed in escrow to be released upon the execution of warrants, whereas for the purposes of verifying ownership of public keys in the case of digital signatures, it is not government, but the parties to the transactions, that require an independent third party to provide a certification or key escrow service for the purposes of holding public keys and being capable of providing a digital certificate authenticating the identity of the owner of the public key to satisfy the requirement of the recipient of the public key.

The US administrations present encryption policy stipulates a considerable number of obligations upon a key recovery agent if it is to be licensed to provide such services and the UK Government's recent proposals for TTP's suggest that they are considering similar levels of obligation. These obligations not only include the fact that the key recovery agent must hand over private keys to Government Officials with lawful warrants but that the key recovery agents should also be independent, of good character and standing, have suitable liability insurance and must accept a relatively high level of liability in monetary terms.

It is understood that a number of potential TTP's in the UK have already commented on the UK Government's proposals by indicating that the levels of responsibility placed upon them are too onerous and inevitably will place undue burdens on competent but smaller TTP's, thereby placing TTP responsibility in the hands of only the largest potential entities. Furthermore, the present proposals in the United Kingdom do not sufficiently differentiate between the roles and responsibilities of a TTP in key recovery situations as against the role of the same entity in relation to the provision of digital certificates and public key authentication.

**OECD/ICC Proposals on Cryptograph Issues**

In the BIAC/ICC "Joint Discussion Paper on International Cryptography Guidelines" submitted to OECD in 1996 in advance of the OECD "Guidelines on International Cryptography Policy" on the 27th March 1997 it was stated:

"International business is demanding seamless webs of communication networks whereby information can flow in a free and secure manner. Secure
world-wide communications are critically important as intruders, criminals, competitors and other unauthorised parties find increasingly sophisticated tools to violate the privacy and security of communications. Business needs internationally accepted means for ensuring the confidentiality, integrity and availability of communications that permit the necessary compatibility of interoperability between different security techniques. Encryption is currently the most appropriate means to secure integrity. An internationally accepted and comprehensive security policy is essential and needed urgently for business to operate in a global marketplace.

The OECD has recently published its "Guidelines on International Cryptography Policy" in which the value of an international PKI is acknowledged but, some doubt is thrown upon such a mandatory system in the case of digital certification but is accepted in principle in relation to key recovery. The OECD Guidelines are precisely that and acknowledge that they can only have real value when they are implemented in national legislation of participating member countries.

The ICC has been actively involved in the area of cryptography issues for many years since clearly cryptography and electronic commerce itself impacts upon international trade and in 1995 set up a specific project to look at the whole issue of electronic commerce (Project E-100). Project E-100 consisted of six working parties, namely:-

- Open account trading
- Electronic credit
- Electronic transport documents
- Legal and regulatory
- ETERMS
- Digital authentication

In April 1997 Project E-100 changed its name to the Electronic Commerce Project and reduced the number of working parties to:-

- Electronic trade practices
- Information security
ETERMS

The objectives of the Electronic Commerce Project are the development of international rules and guidelines for electronic commerce and the development of business services in the field of electronic commerce. Particularly, the Electronic Commerce Project expects shortly to publish its Uniform International Authentication and Certification Practices (UIACP) in order to establish a general framework for digital authentication and certification of digital messages based upon existing authentication and certification law and practice in different legal systems. In so doing the UIACP will provide a detailed explanation of authentication and certification principles, particularly as they relate to information system security issues and public key cryptographic techniques.

The underlying policies articulated and promoted in the UIACP are:-

- To enhance the ability of the international business community to execute secure digital transactions.
- To establish legal principles that promote trustworthy and reliable digital authentication and certification practices.
- To encourage the development of trustworthy digital authentication and certification systems.
- To protect users of the digital information infrastructure from fraud and errors.
- To balance digital authentication and certification technologies with existing policies, laws, customs and practices.
- To define and clarify the duties of participants in the emerging digital authentication and certification system.
- To foster global awareness of developments and digital authentication and certification technology and their relationship to secure electronic commerce.

In addition, UIACP draws upon and extends existing international law treatment of digital authentication in particular that articulated in the United National Model Law on Electronic Commerce (UNCITRAL Model Law).

In addition to UIACP the ETERMS Working Group within the Electronic Commerce Project has developed an electronic repository for the voluntary deposit of standard
terms and messages and contracts used within electronic commerce and it is anticipated that in due course the ETERMS repository may be made publicly available through the ICC Web site currently under development.

Conclusion

Notwithstanding the present lack of a harmonised international policy on cryptography, electronic commerce will continue to grow but its full potential will not be achieved without international co-operation between businesses, individuals and governments in order to bring a balanced solution to the requirements to provide secure and authenticated electronic commerce transmissions whilst preserving the rights of government to monitor such transmissions for the purposes of public policy, preservation of data protection and prevention of illegal acts and terrorism.