BUILDING A TRUSTED ENVIRONMENT FOR E-BUSINESS : A MALAYSIAN PERSPECTIVE

N. M. Din and M. Z. Jamaluddin

Department of Electrical Engineering
College of Engineering, Universiti Tenaga Nasional
norashidah@uniten.edu.my ,mdzaini@uniten.edu.my

ABSTRACT

Almost all studies conducted on network economy and the Internet identify 'security' as a major concern for businesses. In general, the level of security in any network environment is closely linked to the level of trust assigned to a particular individual or organization within that environment. It is the trust element that is crucial in ensuring a secure environment. Besides physical security, security technology needs to be utilised to provide a trusted environment for e-business. Network security components for perimeter defense, i.e., Virtual Private Networks, firewalls and Intrusion Detection Systems, need to be complemented by security components at the applications and user level, e.g., authentication of user. ID or password security solution may be an option but now with the availability of legally binding digital certificates, security in e-business transactions can be further improved. Time and date stamping of e-business transactions are also of concern to prove at a later date that the transactions took place at the stipulated date and time. Digital certificates are part of a Public Key Infrastructure (PKI) scheme, which is an enabling technology for building a trusted environment. PKI comprise policies and procedures for establishing a secure method for exchanging information over a network environment. The Digital Signature Act 1997 (DSA 1997) facilitates the PKI implementation in Malaysia. Following the DSA 1997, Certification Authorities (CAs) were set up in Malaysia. This paper describes a trusted platform for spurring e-business and provides a Malaysian perspective of it.

Key words: Public key infrastructure, Digital certificates, Information security, E-business

1.0 INTRODUCTION

The Internet has bequeathed organisations with opportunities to improve their business processes, target and expand new markets, create business strategies and increase customer satisfaction. However, failure in providing a secure Internet connection may cause financial loss, lost of business opportunities, a tarnished image for service and loss of customer confidence. To participate and to capitalize on the potential of the Internet, having a trusted electronic environment is of vital importance.

For e-sovereignty to exist a trusted environment must be built that will be able to address the issue of information security over an electronic medium. Basically, three main components need to exist for secure communications (Ford and Baum, 1997):

(i) Assurance of the identities of transacting parties
(ii) Confidentiality and integrity of information transacted
(iii) Irrefutability by the transacting parties

Besides physical security, stringent security measures need to be put in place. Network security components for perimeter defense, i.e., Virtual Private Networks, firewalls and Intrusion Detection Systems, need to be complemented by security components at the applications and user level, e.g., authentication of user. ID or password security solution might be an option but can easily be breached, e.g., through brute force techniques. Public Key Cryptography is one of the latest security technologies to offer the level of security required for electronic transactions.

A Public Key Infrastructure (PKI) supports public key cryptography services where a PKI, comprising policies and procedures for efficient key and certificate management in establishing a secure method for exchanging information over a network within an organisation, an industry, a nation or worldwide, exist (PKIX, 2002). The Digital Signature Act 1977 (DSA, 1997) facilitates the implementation of PKI in Malaysia.

2.0 INFORMATION SECURITY

E-business information must be protected both in storage and in transit over the computer telecommunications network. A governing security policy must exist which involves identifying proprietary information and identifying who is allowed to access the information (Cheswick and Bellovin, 1994). Employees need to be advised of threats, countermeasures and their responsibilities in safeguarding information (Forcht, 1994). To uphold the governing security policy, a combination of safeguards in access controls, authentication, encryption and intrusion/misuse detection are required (Ali Yusny and Mohd Aizaini, 2001). Access controls, which include computer and network login controls, firewalls and application layer controls, are essential to prevent unauthorised access to information resources.

Authentication mechanism on the other hand validates the identity of users and other entities including networked computers. Mechanisms include passwords, biometrics, cryptography and digital signatures. Encryption can protect data transmitted over open computer networks and phone lines as well as protect data stored in computers.

Intrusion and misuse detection can be checked through monitoring system behavior, either from audit records or in real time. Software tools are available to detect and eradicate viruses, worms and trojan horses which can be viewed as intrusion detectors. Known vulnerabilities on systems should be addressed, i.e., properly configured and maintained, since intruders will normally exploit these vulnerabilities.

Another component that adds legitimacy and security to e-business transactions is date and time stamping. Digital date and time stamping is required in order to establish and provide evidence as to when an e-business event has occurred, as evident in Datum (2002) and Merill (1999).

PKI is able to provide some of the above safeguards to help organisations improve security in their electronic communications environment. PKI has the capacity to safeguard authenticity, integrity, confidentiality and non-repudiation in transactions (Ford and Baum, 1997).

PKI technology can also be used to authenticate timing devices within a secure hierarchy of clocks and time stamp servers by providing the following three attributes, as discussed in Datum (2002):

i. Assurance that the time came from an official source
ii. Assurance that time has not been manipulated
iii. An evidentiary trail for auditing or non-repudiation.

3.0 THE PKI FRAMEWORK

PKI is an enabling technology for building a trusted environment. PKI uses asymmetrical encryption technology where a widely available key known as the public key is used to encrypt a message. A different key, known as the private key is used to decrypt the message. The private key can also be used to create digital signatures. The private key never leaves the domain of the bearer. PKI enables secure communication between large numbers of users.

The security features found in the public key algorithm as outlined by Stallings (1998) are:

- Authentication. One signs (using the private key) a random generated message/numbers and sends the original message/numbers together with the certificate (public key). The recipient can verify that the message is signed by the sender's private key. Since only the sender has the private key, he must be who he claims he is.

- Encryption (Confidentiality and Integrity). Encryption is usually achieved by using the recipient's public key to encrypt a message. Since only the recipient has the corresponding private key, the message is safe and cannot be read by others.

- Non-repudiation. When a person signs a message using his/her private key, every one can verify the signature with his public key. Since only he could have his private key, he cannot deny signing the message.

PKI incorporating Smart Card and Secure Socket Layer technologies provide an end-to-end solution for building a trusted electronic environment for e-business transactions. A description of the components that are associated with PKI is given below.

3.1 Digital Signature

Digital signature is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of the message or the signer of a document. It can also be used to ensure that the original content of the message conveyed is unchanged.

Digital Signature assures message, document or form recipients that the originator is really who he or she says he/she is. Each individual who wants to transact and/or participate in the Digital Signature processes must be fully and uniquely identified and authenticated. There should be little possibility of impersonation. Each user will be uniquely identified or authenticated by a digital ID sometimes known as Certificates.

3.2 Smart Cards

Smart cards carry an embedded microchip that stores data and applications and in a PKI implementation is used to securely store the digital certificate and key pair (Verisign White Paper, 2001). Smart cards provide a trusted platform that can keep secret keys and cannot be corrupted by viruses or non-authorised software. The smart card requires a PIN for access to the user's credentials, which is an added layer of protection if the smart card itself is lost or stolen.

Smart cards can be used as a digital identity. With PKI the card can be used to enable secure logon, secure e-mail, secure access to proprietary and confidential web sites, or single sign-on to Intranets. Multiple applications can reside on a single smart card, and applications can be added, deleted, or upgraded without reissuing the card.

3.3 Certification Authority

A certification authority (CA) is a trusted source that issues and signs digital certificates. In Malaysia there are currently two CAs, i.e., Digicert Sdn Bhd (Digicert, 2001), the first national CA established in 1998 and Msctrustgate Sdn Bhd. (Msctrustgate, 2001) in 1999. A digital certificate comprises the bearer's public key, digital signature, owner identity, serial number, issuant and expiration date. The purpose of a digital certificate is to provide the bearer with a credential. CA creates, signs and issues digital certificates.

The role of a CA is to certify the veracity and the integrity of the relationship between a public key and the identity of the associated user. The certification processes result in a digital certificate that is used to authenticate and provide irrefutable evidence of an electronic transaction. The verification done by a CA is known as the trusted third party. The public key is a half of key pair, where the other half of the key (Private Key) is kept by the owner. The CA stores the public key in a certificate, which is then signed by the CA as the valid public key. The certificate will be kept in a X.500 directory.

A CA will also maintain the Certificate Revocation List (CRL). A CRL is a list of certificates, which for one reason or another have been revoked before their scheduled expiration date. This may be because the private key has been lost or its security has been compromised. A certificate may also be placed on the CRL if it was issued to a person in an official capacity, which is no longer held.

The process of issuing a certificate requires a high degree of security, comparable to the process of issuing a passport. The CA will authenticate the user and will require proof on the user's identity. Once the user's application has been accepted a key pair (Public/Private) will be generated and the CA will issue and sign a certificate linking the public key to its owner.

Registration authorities (RAs) are elected by CAs to authenticate users based on a set of policies. Cross certification between CAs would enable broader acceptance of the digital certificates from various CAs in business transactions. A CA in Malaysia has to be licensed by the Controller of Certification Authorities in the Ministry of Energy, Communications and Multimedia.

3.4 Secure Socket Layer (SSL)

SSL is a link level protocol that supports server authentication. The SSL protocol is able to negotiate encryption keys as well as authenticate the server before data is exchanged by higher level applications. SSL is the industry-standard protocol for secure Web-based communications (Netscape, 2001).

SSL encrypts all information exchanged between a Web server and a Web browser. This will help avoid hackers from viewing the confidential information. When a message is transmitted over the network, the sending and receiving computers each generate a unique code based on the message content. If a single character in the message content is altered or changed during transmission, the receiving computer will generate a different code, and then alert the recipient that the message has been tampered with.

4.0 PKI DEVELOPMENT IN MALAYSIA

Malaysia has spanned the entire range of issues associated with the legal effect of electronic signatures, the legal framework for the operation of PKI and the establishment of a regulatory body to oversee CAs. Under the requirement of the DSA (1997), the Government is required to establish the controller of CAs, and this has been made in October 1997. The function of this regulatory body is to oversee the establishments and operations of CAs through yearly audit and monthly reporting.

Table 1 shows the licensed CAs, RAs and cross-certification effort in Malaysia to date (Nooritawati, Norashidah and Md Zaini , 2001).

Table 1: PKI Service in Malaysia

PKI Service Type	Service Provider	Year Established
Certificate Authority	Digicert Sdn Bhd	1998
	MSC Trustgate	1999
Registration Authority	Pos Malaysia	1998
	Mimos	1998
	GITN Sdn Bhd	1999
	Sarawak Information System Sdn Bhd	2000
	KKIP Communications Sdn Bhd (Sabah)	2001
Cross Recognition (Certification)	Digicert and Hong Kong Post CA and Singapore Post CA	2000

Initiatives by the government to promote PKI usage can be seen in the e-Government project, i.e., Electronic Procurement and Generic Office Environment. In the electronic procurement project, new vendors and vendors renewing their licenses are given two sets of smart cards which contain certificates and key pairs to perform on-line and real-time transactions with the Government. This will streamline the procurement processes and procedures as well as improve efficiency and productivity. The procurement application, known as e-Perolehan, will require the user to use their e-Perolehan ID Card, which uses a microprocessor smart card, for identification, authentication and verification by the system. The smart card will be storing user profile for each appointed and authorised user and also a Digital Certificate issued by Malaysian Government Licensed Certificate Authority (CA). Only certificates issued by the recognized CA will be used for e-Perolehan. By using the Digital Certificate, all transactions will be considered as legal and valid and every data transaction will be encrypted using 128-bit encryption technology (CDC, 2002).

The MSC's Government Multipurpose Card (GMPC) flagship project will embed a PKI component on the card that will facilitate e-commerce and e-business transactions. The GMPC card or now known as *MyKad* is a smart card that can have multiple-functions for multiple-applications (GMPC, 2002).

4.1 A National Agenda : The Way Forward

E-business in the borderless world will inevitably need to achieve the degree of trust required for types of applications implemented. Else the transacting environment might face possible impersonations of identities and manoeuvring of information in the midst of conducting businesses. Confidence level for doing e-business will not be there, and e-business will be a disaster.

PKI technology is recognized by governments world wide. Argentina, Germany, Italy, Malaysia, Russia and Singapore have enacted legislations regarding digital signatures, and many other countries, such as Australia, the United Kingdom and United States have made official studies and proposed legislative initiatives.

PKI is still in its infancy in Malaysia as it is in the rest of the world. However, the seriousness of the government is lauded by being one of the first countries in the world to enact legislation on digital signature. In Malaysia, PKI solutions have a firm footing as compared to other technologies in offering secure communication since the digital signature legislation is behind it.

In line with the legislative efforts in Malaysia, PKI technology looks set to be the solution for a trusted e-business environment. With PKI, businesses have the backing of the enacted law. However, PKI is an infrastructure and as such is only worth as much as the applications that can operate within its framework. Efforts on developing PKI based applications are required. Examples of applications that can be used for PKI implementations include e-mail, messaging, on-line services for B2C and B2B e-commerce.

4.1.1 Issues related to PKI implementation

Movements towards establishing standards between PKIs in Malaysia need also take consideration of PKIs in Asia and the rest of the world so that the use of PKI can be capitalised across the borderless internetworking world. A technological barrier that needs to be overcome is the interoperability between PKIs. PKIs are semi-proprietary in their standards and basic infrastruture, e.g., one PKI implementation can have multiple roots and another can have a single root. In Malaysia, for instance, Digicert Sdn. Bhd. and MSC Trustgate.com are using different technology in their PKI implementations. Digicert operates using a single root where this root is maintained by Digicert in Malaysia while Msctrustgate is having their root signed by Verisign, Inc. located in Mountainview, USA. An additional concern is that PKI standards have yet to be established to enable multiple PKIs to interoperate and multiple applications to interface with a single PKI.

Another technological barrier is that the Internet standards and formats in PKI are considered too heavy for mobile implementation with low processor and memory capacity. The X.509, which is the standard certificate format, is too large to send over the air (500 bytes to 1K) and users may have to end up with, large storage requirements if several certificates are required. However, if a new format is used, incompatibility with the existing wired PKIs will arise and wired and wireless users will have separate PKIs. The CAs in Malaysia have yet to announce any wireless specific services. Elsewhere in Asia, movements towards establishing a wireless PKI standard can be seen such as in Korea and the formation of the Asian PKI Forum (Report of PKI Forum, 2001).

Issues of time stamps for e-business transactions need to be addressed. The digital date and time stamps framework and implementation must be able to stand up in the Malaysian court of law.

E-sovereignty implicates national security and foreign involvement needs to be checked. In the wake of September 11, 2001 tragedy, United States lawmakers are calling for laws that will make it easier to crack encrypted messages by creating a "back door" in their encryption products. Furthermore some countries, e.g., Canada and the US, control exports of encryption programs on the basis of foreign hostile organizations and governments using it to communicate secretly. This can be seen in the Wassenaar Arrangement (Wassenaar, 1995), where export restrictions have been imposed on strong cryptographic software.

Having a foreign CA might jeopardise national security. One policy under debate in the US is mandatory key recovery where law-enforcement and intelligence agencies would hold keys for decrypting any electronic communication. Licensed local CAs should be in control of the technology, e.g., management of the PKI key pairs, in order to avoid undercover surveillance and foreign elements in the PKI enabling products.

5.0 DISCUSSION

The government and the private sectors need to work together to address legal, trade control and security-related issues that may be impeding the use of e-business.

To facilitate the demand for PKI based applications, skill sets pertaining to PKI systems integration and maintenance need to be developed. Courses related to computer security and PKI need to be established and expanded in institutions of higher learning to support the e-business development. Research and development activities should address PKI related issues so as to ready and propel Malaysia into the e-business scene. The government's Multimedia Super Corridor flagship applications, for instance, can be a catalyst to the promotion of a trusted environment in e-business applications to make them reliable world class show case applications. To this end the Malaysian government can play a leadership role by ensuring that a legally trusted environment is a feature of their pilot applications

6.0 CONCLUSION

Transacting in the borderless cyber-world requires safeguards. PKI is seen as a technology that could play a part in establishing e-sovereignty, i.e., secure transactions over the internetworking-computing environment. PKI provides security in the form of authentication, confidentiality, integrity and non-repudiation. PKI are recognized by governments world wide and given consideration in their legislative initiatives and supported legally in Malaysia.

Without a trusted environment electronic transactions may be obscure and suspect. In order to unlock the Internet economic potential and not lose out in the borderless digital economy, Malaysian businesses would need to plunge into e-business. Organizations can employ PKI according to their e-business needs. A national agenda should include forums to promote the awareness of the security technology available, besides addressing the issues involved in implementing and improving the technology.

REFERENCES

Ali Yusny Daud & Mohd Aizaini Maarof (2001). Application Framework for E-Business: E-Business Security Requirements. In Proceedings of *the 2nd Conference on Information Technology in Asia,* 288-299. Universiti Malaysia Sarawak.

Cheswick, W.R., & Bellovin, S.M.(1994). *Firewalls and Internet Security.* Reading, Massachusetts.

Datum (2002).*Time Stamping*. http://www.datum.com/tt/trustedtime/index.html.

CDC (2002). http://www.commercedotcom.com. my/.

Digicert (2001). http://www.digicert.com.my.

DSA (1997). *Digital Signature Act.* http://www.mycert.mimos.my/.

Forcht, K. (1994). *Computer Security Management.* Course Technology, Cambridge.

Ford, W., & Baum, M.S. (1997). *Secure Electronic Commerce*, 94, New Jersey.

GMPC (2002). http://www.jpn.gov.my/gmpc/index.htm.

Kaeo, M. (1999). *Designing Network Security*, 158, Indianapolis: Cisco Press, Macmillan.

Merill, C. B.(1999). *Time is of the essence: Establishing the critical elements of electronic commerce*, http://www.pkilaw.com/surety_time_long_3.htm.

Msctrustgate (2001). http://www.msctrustgate.com/.

Netscape (2001). *Secure Socket Layer*, http://home.netcape.com/security/tech-briefs/ss1.html.

Nooritawati Md Tahir, Norashidah Md Din & Md Zaini Jamaluddin (2001). Development of Public Key Infrastructure Implementation in Malaysia. *Proceedings of the International Conference on Information Technology and Multimedia at UNITEN*, Recent Advances and Future Trends in Information Technology and Multimedia, Universiti Tenaga Nasional.

PKIX, (2002). Internet X.509 Public Key Infrastructure: Roadmap, http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-07.txt.

Report of PKI Conference (2001). *Korea PKI Scheme and PKI Policy and Framework in Korea,* PKI Conference, Ministry of Information and Communication, Seoul, Korea.

Stallings, W. (1998). *Cryptography and Network Security*, 9-11. Prentice Hall.

Verisign White Paper (2001). *Extending Managed PKI Services to Smart Cards for Greater Convenience and Security.* http://verisign.com/products/smartcard/SmartCard.pdf.

Wassenaar (1995). http://www.wassenaar.org/.