The control implications of a public key infrastructure

A Bouwer

School of Accountancy
University of Pretoria

Abstract

Organisations continuously have to question traditional thinking and implement state of the art systems to control e-commerce applications. A Public Key Infrastructure (PKI) has established itself as the generally accepted method to control e-commerce transactions. This infrastructure comprises complex technology supported by specific manual and electronic control procedures. In the e-commerce realm, auditing professionals are increasingly challenged with new technologies and different methodologies such as PKI. This article examines the inherent risks associated with implementing a PKI and gives guidance on control appropriate control measures.

Key words:
audit, e-commerce, control, public key infrastructure, digital signature, digital certificate, public key cryptography, public key, private key.

1 INTRODUCTION

The Internet is rapidly slashing costs between suppliers and companies, and between companies and customers. As it creates entirely new businesses and realigns old ones, it is scrambling notions of corporate value, giving rise to a new business math that remains volatile but increasingly draws from real numbers about sales, productivity and even profits.

During June 1999, after perhaps the most comprehensive study undertaken on the subject, funded by network equipment maker Cisco Systems Inc., researchers at the University of Texas said the Internet generated about $301 billion in U.S. revenue in 1998 – thus closing in on the automobile industry earnings. Business-to-business commerce alone is likely to swell thirty-fold, from $48 billion last year to $1.3 trillion in 2003, according to technology consulting firm Forrester Research Inc. Forrester estimates that consumers spent $8 billion buying computers, books, CDs, clothing and other items on the Internet during 1998 (Leibovich, Smart & Dugan 1999:A1).

The same trend was experienced in South Africa during 1999 with exceptional growth in Internet users and various mergers and shake-outs in the Internet Service Provider (ISP) market. Many local businesses are also increasingly using the Internet to conduct electronic business. Leading the transition from traditional business methods to e-commerce, in both the local and overseas markets, is the financial services industry. Banking online, real-time stock trading and obtaining insurance on the web are no longer exceptional occurrences, even in South Africa.

Although the growth in e-commerce can be described as astonishing, security over messages sent across the Internet remains the single most import barrier to even greater growth figures. Executives are concerned about Internet security and many organisations have experienced security breaches. This has caused many businesses to be wary of following the e-commerce trend (Bouwer & De Jager 1998:23-25).

Attempts to secure the Internet have focused largely on securing the medium itself through the combination of the Internet, private leased lines and internal networks. This is prohibitively expensive and, in some cases, infeasible for potential parties to a transaction. The limited success achieved through these methods lies at the root of executives' concern and resistance to e-commerce. For the Internet to offer an inexpensive and ubiquitous solution, the focus must be on information security. In order for it to serve our purposes as a vehicle for legally binding transactions, efforts must be directed at securing the message itself, as opposed to the transport mechanism (American Bankers Association 1999:2).

The solution in providing the security required by electronic commerce has been found in the implementation of a Public Key Infrastructure (PKI). A PKI uses digital signatures to offer the ability to encrypt messages sent across the Internet while the integrity of the message content and the validity of the sender can be verified through the use of digital certificates. When implemented and used correctly and controlled appropriately, a PKI can effectively secure e-commerce.

2 IMPLEMENTING A PUBLIC KEY INFRASTRUCTURE

In order for an organisation to implement a PKI, the first phase comprise of the installation of digital signature software. Through the use of public key cryptography, this software will enable the organisation to generate a private and public key pair and release its public key to the online world.

This process facilitates the attachment of digital signatures to messages. Digital signatures are an actual transformation of an electronic message using public key cryptography. Through this process, the digital signature is tied to the document being signed, as well as to the signer, and therefore cannot be reproduced. Public key cryptography involves an asymmetric key pair. This key pair is comprised of what is referred to as a public key and a private key. The public key, as its name suggests, may be freely disseminated. This key does not need to be kept confidential. The private key, on the other hand, must be kept secret. The owner of the key pair must guard his private key closely, as sender authenticity and non-repudiation are based on the signer having sole access to his private key.

These key pairs have several important characteristics. First, while they are mathematically related to each other, it is impossible to calculate one key from the other. Therefore, the private key cannot be compromised through knowledge of the associated public key. Second, each key in the key pair performs the inverse function of the other. What one key does, only the other can undo (American Bankers Association 1999:4).

The public key on its own, however, gives no guarantee regarding the key's authenticity. This problem will be addressed during the second phase of a PKI implementation. This phase involves the implementation of digital certificates. Since digital signatures do not provide authentication of the originator of a message, a significant risk still exists that invalid or “spoofed” messages are received. This scenario underscores the need for some type of entity to serve as a trusted third party (TTP) to vouch for individuals' identities, and their relationship to their public keys. This entity, in PKI terminology, is referred to as a certification authority (CA).

The CA is a trusted third party which issues digital certificates to its subscribers, binding their identities to the key pairs they use to digitally sign electronic communications. Digital certificates contain the name of the subscriber, the subscriber's public key, the digital signature of the issuing CA, the issuing CA's public key, and other pertinent information about the subscriber and his organisation, such as his authority to conduct certain transactions. These certificates have a default life cycle of one year, and can be revoked under certain conditions such as private key compromise or separation from an organisation.

These certificates are stored in an online, publicly accessible repository. The repository also maintains an up-to-date listing of all the unexpired certificates which have been revoked, referred to as a certificate revocation list (CRL). The repository also maintains an electronic copy of the certification practice statement (CPS) of each CA that publishes certificates to it. The CPS outlines the policies and procedures of each CA's operations from registration of a subscriber to the physical security surrounding their CA system (American Bankers Association 1999:4).

3 CONTROL OVER A PUBLIC KEY INFRASTRUCTURE

A PKI is in essence implemented as a control measure to secure messages sent across the Internet. There are, however, certain important risks associated with this technology which, if not managed carefully, could leave an organisation exposed. As with most new technologies, the biggest risk is that management could be unaware or uneducated regarding the impact of implementing such technology. As will be shown, the impact of some of these risks can be severe and auditors in particular have a duty to identify weak PKI's and bring these risks to the attention of their clients.

The most important risks associated with a PKI are discussed below. These risks are not the only risks to be found in a PKI environment nor are they unique risks. They do, however, alter the risk profile of an organisation which has implemented a PKI and are therefore important to auditors who need to evaluate the internal control of such an environment.

- Physical security of personal computers (PCs).

Once a PKI has been implemented, the PC is both much more vulnerable and more desirable to criminals. Since the digital certificate and digital signature are in most cases stored on the PC's hard disk, access to the physical PC affords the criminal the opportunity to transact on behalf of the legal owner of that PC. That digital certificate can be likened to a passport and will be accepted as valid by all the organisation's trading partners.

To worsen the scenario, most PKIs attempt to facilitate the digital signing process transparently with little or no human interface. Digital signatures are by default attached to messages sent in a PKI (InterClear 1999). This has the effect that a criminal does not even need a password to send a message with a valid digital certificate attached to it.

Although organisations traditionally encourage the use of PC passwords such as Windows passwords, it has not seriously been enforced since the majority of an organisation's PCs contained very little valuable information. In fact, users are normally discouraged from keeping critical information on PCs since it could more easily be lost than on a mainframe or server. It is therefore crucial that the organisation's attitude to this changes. When evaluating an organisation's PKI, auditors should establish if the access control over the organisation's PCs has been enhanced to cater for this increase in risk. A user awareness campaign should also have taken place to ensure that users' traditional attitude towards PC access control change accordingly. More emphasis should also be placed on application level passwords, in this case passwords to the browser or mail client used to send Internet messages. In very sensitive PKI environments the use of smartcard readers, to keep the digital signatures and digital certificates off the PC and on a smartcard, might be called for.

- Managing digital certificates.

Once a PKI has been implemented by an organisation, it has to be decided which individuals in the organisation are entitled to certificates and what authority they have to use them. If this is not managed properly it could lead to disaster. It could be likened to the issuing of company credit cards to employees. Only authorised personnel should get them, limits should be set and cards should be cancelled when lost or if the employee leaves the company. In the case of digital certificates an additional risk exists. If a digital certificate is lost or deleted none of the messages originally encrypted with that specific certificate attached can be read again (InterClear 1999).

In a PKI the issuance of digital certificates should therefore be planned in accordance with the organisational structure and approved at an appropriate level. If any messages sent with a digital certificate form part of an audit trail or need to be referred to again, provision must be made for the backup of those digital certificates to ensure that historic messages will in future be readable.

- Access to PKI data.

Most PKIs in an organisation are managed centrally. From this server digital certificates are issued and updated or deleted when necessary. The obvious risk is that unauthorised access to this function could result in the issuing of unauthorised digital certificates, the changing of authority levels or the destruction of valid certificates. It must therefore be ensured that strict access control to the PKI server is in place and enforced.

- Access to private key.

A digital signature is only effective insofar as its private key can be protected. Even when the use of a PKI application on a PC has strong password protection, it is possible for a hacker to find the private key stored on the PC's hard drive. Various software debuggers are available on the market which enable a hacker to follow the process flow of a program. When the program calls for the private key to encrypt or decrypt any message the debugger detects this and the key has been exposed. Although this procedure calls for above average computer skills, it is common knowledge for experienced programmers.

The only effective control against this type of attack is once again the physical protection of PCs. In PKIs where very sensitive or critical data is transmitted and stored, management must be aware of this threat and implement strict physical and logical access controls or even smartcards if appropriate. The use of digital certificates on notebooks, which are more prone to be taken out of the controlled environment, should also carefully be considered.

- Reputation of the Certification Authority.

A Certification Authority (CA) plays a crucial part in the successful implementation of any PKI. This authority acts as a trusted party and once such an authority has given its stamp of approval to a message, the message will be accepted as authentic. An organisation must therefore ensure that it does not deal with a wolf in sheep’s clothing. Management must scrutinise the CA’s reputation, track record and financial stability before appointing the CA as a trusted third party. A legally binding contract between the organisation and the CA must also be signed, giving the organisation legal recourse in the event of a breach of contract.

- Legality of digital certificates

In the United States, the legal presumptions involved in relying on a properly verified digital signature are that the message is presumed not to have been altered since sent, and that the signature is presumed to be that of the named signer. Furthermore, a digitally signed electronic message meets all "in writing" and signature formalities, and is considered to be the original (American Bankers Association 1999:4). In the United Kingdom, as in South Africa, a digital signature currently has no legal status. The UK government has, however, indicated that it will enact legislation giving a digital signature the same status as a handwritten signature and will equally legally bind parties to an agreement. (InterClear 1999).

The implication of the current legal standing in South Africa is therefore uncertain and organisations should not rely on digital signatures or certificates alone in the case of material agreements. In practical situations digital signatures must subsequently be backed up by handwritten signatures before significant resources are spent on contracts above a material amount.

4 CONCLUSION

Public Key Infrastructures are here to stay. A successful technology can in most cases be recognised by its general acceptability, which PKIs have already proved by their present implementation in many of the world’s biggest companies. What is even more astonishing is the fact that only one standard, namely public key cryptography, exists (Bishop 1998).

Auditors must therefore understand this environment thoroughly not only to determine the appropriate audit risk but, importantly, to also successfully guide their clients through the implementation of a PKI. Certain risks in a PKI environment could alter an organisation’s risk profile dramatically and, if left uncontrolled, could lead to material financial losses.

It has been shown in this article that various controls, varying in technical complexity, must be implemented in a PKI environment. Auditors could therefore be intimidated by the complexities of cryptography and the digital verification processes. Basic auditing principles will, however, prevail in this environment. Even if an auditor ignores all the technical issues in a PKI environment, his or her most important function is to instruct the client on the important risks associated with a PKI and to ensure that proper processes are put into place to address those risks.

References

American Bankers Association. 1999. Digital Signatures: *The Key to Information Technology Security*. ABA.com White Paper. (http://www.se-com.com/secom/docs/chapter5-0.html)

Bishop, B. 1999. Certificate of Authenticity. *CIO* Magazine. July 15, 1998. (http://www.cio.com/archive/071598_et.html)

Bouwer, A.M. & De Jager, H. 1998. Internet firewall environments: an audit perspective. *The Southern African Journal of Accountability and Auditing Research*. Vol. 1: 1998.

InterClear. 1999. Frequently Asked Questions. (http://www.interclear.net/FAQ)

Leibovich, M., Smart, T. & Dugan, I.J. 1999. Internet's E-conomy Gets Real. *Washington Post*. June 20, 1999. (http://www.washingtonpost.com/wp-srv/business/daily/ june99/internet20.htm)