2

CERTIFICATE BASED PKI AND B2B E-COMMERCE: SUITABLE MATCH OR NOT?

Kok Ming Ang
Information Security Research Centre
School of Data Communications
Queensland University of Technology
km.ang@ieee.org

William J. Caelli
Information Security Research Centre
School of Data Communications
Queensland University of Technology
w.ceelli@qut.edu.au

Abstract This paper proposes that an urgent re-evaluation is needed to assess whether or not X.509 certificate based structures are the best technology to implement security schemes for business-to-business (B2B) electronic commerce operations. In particular it proposes that alternative structures based around simplified directory schemes and "trading partner agreements" and other concepts offer far more efficient and scalable solutions. In addition, directory structures and associated legal agreements provide a better solution to the problem of evidentiary collection and presentation in the case of disputes, particularly where these involve legal proceedings. Far more work is needed on the mirroring in information systems and data networks of the time-honoured practice of involvement of a "notary" or "witness" to an important set of transactions, such as those relevant to the B2B environment. This is markedly different to the business-to-consumer (B2C) situation involving much smaller level transactions. Overall, however, the need for trusted computing environments (such as those based around "mandatory access control" schemes) is paramount in building trust in any computer/data network scheme involved.

1. INTRODUCTION

Public key infrastructure, in support of electronic commerce, based on X.509 certificates concepts and allied technology has been extensively studied by researchers (Berkovits et al., 1994; Ellison and Schneier, 2000). However, some problems are quite visible, and many researchers have sought to use cryptographic protocols to repair flaws. Electronic media do not have the distinct features of traditionally signed paper records. Multiple digital copies are indistinguishable from each other while paper documents can be made and recorded with unique, highly unalterable characteristics Moreover, the act of signing is itself surrounded by "ceremony" often involving one or more witnesses. Moreover, the "signer", in approving the contents of a document through affixation of a signature, mark and/or seal, has reasonably complete knowledge of the total contents of the document to be signed and complete control over the signing process. In the case of B2B electronic commerce, problems clearly exist in these areas, particularly if commercial-off-the-shelf software systems are employed with little to no knowledge of their content or operation. These well established and legally tested processes are precisely the problems that, in many important areas such as wills and testaments, real estate titles, court records and so on, prevent electronic records from gaining complete legal recognition. Current dependence upon digital certificate structures appear to be not relevant to the solution of these important and legal requirements for trust in signing.

2. WHAT COMMERCE NEEDS

Electronic technology can satisfy business and legal requirements for the conduct of national-level and international commerce. The basic function of any electronic commerce scheme must be the ability to, at a minimum, mirror the reliability, security and trust levels developed over time through traditional commercial activities and accepted practices.

Any security scheme for B2B electronic commerce must properly address the underlying concern for business certainty. Not only does it need to cater for normal business activities, such as reliable delivery of ordered products, dependable payment mechanisms, etc, but on also the ability of the business partners to be able to resort to applicable law should a dispute occur. Traditional and accepted security mechanisms like paper trails and availability of records, business auditing, agreed contracts and signature witnessing serve to reinforce trust and certainty by provision of credible evidence of normal business practice.

Trust is an often-used but vaguely defined term. One crucial aspect is the involvement of human perception and emotion, which cannot be merely defined with mathematical or scientific rigour.

2.1. TRADITIONAL ELECTRONIC COMMERCE (EDI)

Electronic Data Interchange, or EDI, has been a strong business tool for almost three decades in a number of differing forms (Kimberley, 1991). B2B electronic commerce is just another manifestation of exactly the same business desire to more effectively perform business functions for inter-company trading while minimising the costs involved. B2B is one aspect of the broader electronic business "triangle" as shown in Figure 1.

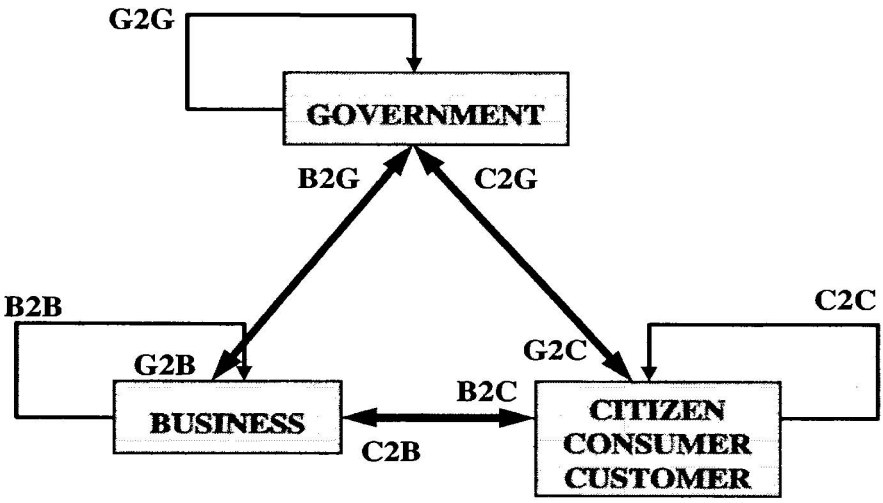

Figure1 Electronic Business Participants

B2B electronic commerce may thus be envisaged as the latest manifestation of EDI whereby trading activities are carried out over the Internet, using its protocol suite, and because of the lowering of costs involved, now includes small to medium scale enterprises. These were often unable to avail themselves of the earlier EDI structures due to cost limitations. It should be noted, however, that other, more specialised forms of EDI have existed for a long time in specific industries such as the banking and finance industry (through EFT or Electronic Funds Transfer), etc. Kimberley (Kimberley, 1991) describes the bases of EDI as follows:

> "The basic principle of EDI is that computer-generated trading documents, such as orders and invoices, are transmitted directly to a company's trading partner's computers across a telecommunications network. The term trading partner is used to describe any company, government department, or commercial or non-

> government entity with whom an organisation regularly exchanges documents containing formatted data (i.e. not just memos or letters) as a normal consequence of carrying out business or governmental functions."

The important principles identified by EDI include the concept of "trading partner" and the use of agreed standards for formatted data transfer.

3. BACKGROUND

EDI systems have been in place for almost two decades, particularly in Europe. Standards have emerged for their use. In particular, standards for electronic document content are vital for inter-operability, although even in the "paper world" standards assist greatly as was demonstrated (Kimberley, 1991) during the great Berlin airlift after World War II. In the USA the need for more "global" transactions standards across industries, was recognised as early as 1978 with the formation of the ANSI X. 12 committee. However, elsewhere, other routes were taken. In particular, the formation of the United Nation's EDIFACT group in the mid-1980s was a culmination of over 10 years of work by that international organisation on facilitation of international trading procedures, that again owe their origins to the late 1940s. Standards derived in this manner found their way into the ISO scheme.

However, it is important to note that the need for security in the form of document authenticity, integrity and privacy was recognised in these EDI activities. While technological solutions were defined and the use of X.500 style directories were seen as the logical structure and place for storage of and access to required cryptographic keying materials, the use of a "Trading Partner Agreement" formed a basic concept in legal acceptance of the scheme. These agreements, which it may be argued, should still play a major role in any B2B arrangement since they give force to partner desires to trade electronically and provide a base for reconciliation and resolution should problems occur, as they invariably will.

4. HANDWRITTEN AND DIGITAL SIGNATURES

The use of the term "digital signature" in (Diffe and Hellman, 1976a) and (Diffie and Hellman, 1976b) coupled with a short explanation of the concept involved started a search for an electronic replacement for the human handwritten signature, as a verifier, through the use of the then newly re-discovered "public key cryptography" concept. However, there are significant physical and legal differences between a normal "signature" and the term "digital signature" such that the latter is not, it is contended in this paper, a straightforward replacement for use in electronic commerce.

4.1. DEFINITION OF SIGNATURES

A traditional signature is given as a mark impressed upon paper with a pen or other mechanical seal (McCullagh et al., 1998). One legal dictionary defines it as (Nygh and Butt, 1997):

Signature A person's mark on a document which indicates his or her intention to be bound by its content.

Testamentary Signature A testamentary signature may include the specific mark or initials of the testator as well as his or her name. The test for validity of the signature is whether what has been written was done by the testator as an authentication of what precedes it as his or her will.

It must be provable in a court of law that the mark is affixed with such instruments by the signing person or under his or her authorisation. In this sense, there are some notable physical and legal differences between "autographs", "signatures" and "seals". A handwritten signature is a human biometric action controlled and explicitly performed by an individual, while a seal is a physical token wielded by its owner. An autograph, interestingly, while physically resembling a traditional biometric "signature", is not a strict signature since there is no intention by the "signer" to be bound by any agreed document or the like. In addition, the legal recognition of "seals" also varies with different jurisdictions (McCullagh et al., 1998).

Assuming that "digital signature schemes" are implemented in a reliable and a reasonably trustworthy manner, complex calculations such as '$x^y \bmod n$' (modular exponentiation) and message or data "hashing" are not done using mental arithmetic by a potential "signer"[1]. The user has limited to no control over, and normally no knowledge of, the processes involved in the actual imprinting or "signing" act and it is therefore more logical and appropriate to rename this process as that of affixing a "digital seal". In this sense, the end user has no idea as to whether or not a digital signature created is correct at the time of affixation. He or she must have complete trust in the program used to create the digital seal and in the correct contents of computer memory at the time the "document" is "signed" or "sealed". For example, in the case of a typical home personal computer it is unreasonable to make this assumption since such systems, both hardware and software, were never designed with security requirements in mind at all.

Verifiable "digital signatures" fall under the legal definition of a more general term "electronic signature", which includes non-cryptographic markings such as digitised images and facsimiles of handwritten signatures, typed names, and

[1] This refers to the commonly used RSA digital signature exponentiation calculation.

electronic mail address headers (ABA, 1996). While electronic signatures are trivial to copy, human autographs are relatively harder, but not impossible to forge. Additional protective mechanisms have developed over time to combat handwritten forgery, such as the vital legal process of "witnessing".

4.2. SIGNATORY EVIDENCE

In a law court, a signature on a paper document can either indicate a willingness of the signer to be bound by the document's content or the signer's authorship. This reliability of handwritten signatures as evidence is premised on the following assumptions (McCullagh et al., 1998):

- The signature leaves a semi-permanent mark upon the medium and cannot be easily removed without leaving any sign of alteration.
- The signature design of the person is expected to be relatively unchanging.
- The signature, or together with a printed name, can sufficiently identify the signer.

Digital media record every single bit faithfully and permit easy changes. Thus, electronic images of handwritten signatures are easily copied and unreliable and need cryptographic digital signatures coupled to them to produce a unique and unforgeable mark. Still, a digital signature on a message can be easily removed with a text editor or word processor and substituted with another different recalculated signature. This is in sharp contrast to paper, where no two signatures are exactly identical and therefore a person can be identified with his or her relatively unchanging signature pattern. Moreover, physical removal and/or substitution of a "paper signature" is still not a simple matter, even given modern imaging systems.

A digital signature is not immediately verifiable by visual inspection; its public key is required to recompute the signature from the message for verification. In turn, the public key is dependent upon its corresponding private key. The user can either claim that his private key was compromised without his knowledge and an adversary signed with his private key, or he did not authorise a computer program to sign on his behalf and the computer system did so contrary to his desire.

4.3. WITNESSING

The traditional "notarisation" process serves to counter fraud, signature forgery and repudiation (McCullagh et al., 1998). A "notary" is normally a person physically present at the act of signing to witness the physical action of the signer putting to paper an identifying mark in full knowledge of its intent, and at the same time observe the physical/psychological state of the signer and

the circumstances surrounding the act. Shortly after the signing, the notary at the scene places his/her "autograph" on the same paper as a sign of witnessing the person's act of signing. In the event of dispute, the paper is admissible as evidence in a court of law and the notary can be called to testify on the witnessing of the signature process.

"Digital notarisation services" provided by PKI vendors are vastly different from this traditional process. For example, Verisign's "Validation Services" apply a digital signature and time-stamp on the document (Verisign Inc., 2000). Strictly speaking, it is conjectured that the person who is the alleged holder of the "private key" to be used for digital signing purposes, authorised a program to sign a document using that key and a third party applied another digital signature and time-stamp to the supposed signed document. Using untrusted or unreliable computers, there is a lack of reasonable proof that a document was willingly and deliberately signed by the alleged originating party, and the vendor's authorisation marks were applied to the correct document.

Alternatively, a human notary can be physically present at the act of digital signing and apply a witnessing signature (McCullagh et al., 1998), but the lack of "trusted systems" at the home/small business and commodity computer level, again brings into question the legal validity and certainty of such actions. It appears obvious that any usage could be reasonably open to challenge in a court of law in the case of dispute. Neither side to a court action could present irrefutable evidence that the computer systems used was reasonably protected against tampering, insertion of "Trojan Horse" or "viral" programs, untrustworthy or unreliable software sub-systems, protection of the signing process and the associated cryptographic keys, etc.

4.4. CEREMONY

The process of signing on physical medium carries a cautionary purpose. The signer's attention is brought to the gravity of a document's contents and its likely legal consequences (Jueneman and Robertson, 1998, pp. 430-431). By signing the document, the person is presumed to have understood its contents and is therefore willing to accept its terms. The psychological burden is more pronounced in the presence of witnesses and is often adequate to deter hasty signing. Even with seals, such as usage in the case of "deeds", etc., this ceremonial importance in contract approval is notable. In the earlier case of EDI, mentioned above, this ceremonial function was largely taken up by the legally binding "Trading Agreement" that covered all activities between the parties to an EDI scheme.

It could be argued that frequent users of computers and similar devices have developed "Pavlovian" behavioural characteristics such as repetitive clicking on graphical window menu items and buttons (Sneddon, 1998), particularly where

the consequences of the action are incompletely understood and the underlying technology base is “foreign” to them. Automated batch programs and command scripts are also used to take the drudgery out of predictable computer input and responses. Unlike writing a autograph, there is a lack of ceremony in using computer interfaces for digital signing. This comparative social difference may be contested by users who are not aware that an act of signing has been inadvertently committed on their behalf.

4.5. BURDEN OF PROOF

Under the common law, a person has the right to deny a signature that is attributed to him or her (McCullagh and Caelli, 2000). The fact-finder or “relying party” will have to supply sufficient evidence to prove the signature’s authenticity or the valid circumstances surrounding the signature's formation.

However, legislation on “electronic: transactions” appears to have taken a different step. The United Nations Commission on International Trade Law (UNCITRAL) Article 13 (McCullagh and Caelli, 2000) and the Utah Digital Signature Act (Biddle, 1996) attempt to shift the burden of proof onto the signer. This departure from traditional legal norms does not account for a number of problems.

In traditional signing, the signer has total control over his or her signing action and does not need to worry about any other mechanism that may falsely insert, steal or record the signature2. On the other hand, in the electronic case, computer viruses, smartcard physical theft or computer hacking can compromise the signer’s private key, a vital component of the signing process. Under the Utah Act, the signer must prove that the signature was not affixed by himself or herself and sufficient duty of care was exercised, although the Utah Act remains silent on what constitutes reasonable care (Biddle, 1996).

Recent legislation on electronic commerce such as the E-Sign Act (E-Sign Act, 2000) accord legal recognition upon electronic records and signatures. However, the inconsistent recognition of non-repudiation issues between paper and electronic records may hamper the paper-to-electronic commerce transition, or even electronic commerce across different social-legal borders.

5 . MISCONCEPTIONS

The words “digital” and "electronic" are frequently used interchangeably. As a result, many laymen are confused over the differences between digital and electronic signatures, and policy makers often mistake the former definition for the latter. Nevertheless, digital signatures are still different from the traditional

[2]Although carbon paper can also duplicate signatures, it is relatively easy to detect its use. (McCullagh and Caelli, 2000)

version. Even with biometrics incorporated into digital signature processes (Jueneman and Robertson, 1998) and associated timestamping techniques, these do not have the affirmative features of witnessed, written signatures. A digital signature (or seal) cannot be equivalent to a written signature (Harbison, 1998, p. 114), even if laws are passed to try to make it so.

5.1. THE PURPOSE OF CERTIFICATION

An original proposed application of public key cryptography was to create a secure directory service to assist communication privacy between users and prevent impersonation attacks (Diffie and Hellman, 1976b; Kohnfelder, 1978). This required a user to contact an opposite party, pause communication while the pertinent public key of that opposite party is retrieved from a directory and then verified, and then proceed on with secure communications, which was inconvenient (Kohnfelder, 1978, p. 39). In addition, the administrative burden of maintaining a large, secure, database of people's public keys is difficult. Hence, the concept of "digital certificates" was proposed and designed to reduce the need for frequent public key retrievals and associated directory updates.

However, Kohnfelder also admitted that certificates would not provide any extra benefit when the directory is compromised or users frequently lose their keys (Kohnfelder, 1978, p. 42). In these situations, the costs of certificate revocation outweigh the benefits of certificate use. This is contrary to the belief that certificates provide ". . . a scalable and secure method (from an integrity perspective)" to distribute public keys (Adams and Lloyd, 1999, p. 74). Certificate may even add a greater administrative burden for directories maintenance and users with little to no advantage at all.

5.2. DIRECTORY SERVICES

Directories are not suitable for holding, or ever intended to hold, the private cryptographic keys used for digital signing purposes. They were originally meant to store communications secrecy keys, such as "session keys", and not signing keys (Diffie and Hellman, 1976b). When a directory user dials a wrong telephone number or sends an encrypted message to the wrong person, it is merely an inconvenience. Nobody sues a telephone directory publisher for wrong information (Landrock, 1999, p. 411), because there is no associated legal burden.

5.3. UNTRUSTED COMPUTING

One major problem common to all security woes is the lack of trustworthy and reliable computing systems (Thompson, 1984; Anderson, 1994b; Anderson, 1994a). The functions of a secure information processing system requires authentication, authorisation and detection and compensation of non-orderly

behaviour including software and hardware reliability and human behaviour (Dierstein, 1990).

A computer system, or its cryptographic software, may be compromised by viruses or Trojan horses with no tell-tale signs. Private keys or pass-phrases to these keys can be stolen and be used to falsify document authenticity. Flaws in computer hardware, operating systems and cryptographic software become a burden on the end user. Without any legal liabilities at present, manufacturers see little need to take remedial steps and to offer high-trust commodity computer systems. Computer hardware manufacturers and software houses are not mentioned in legislation as maintaining any liability, and legal disclaimers place the risk of computing systems onto users.

It is almost impossible to dictate user key management practices (Anderson, 1994b; Davis, 1996). Responsibility for the protection of a user's private key, essentially their "digital identity", lies solely with the user. This is clearly unreasonable where available computing systems and the public key certification systems does not adequately address the needs for higher level access control, such as "mandatory access control schemes".

Fraud does occur with paper based B2B commerce systems, but control mechanisms have been developed over time by society, governments and the legal system to deal with it. Although it is trivial to forge letters, paper audit trails and extensive record keeping help reduce forgery. An executive within a company can exceed his or her powers and perform an unauthorised and potentially illegal transaction on behalf of the company. In a court of law, the organisation of the executive is responsible for the said transaction, and, in turn, could press criminal charges against the erroneous executive.

There is no trustworthy path from the user to the end of the communication path. Paper-based systems employ paper trails and audit practices, while digital signing processes lack such multi-faceted structures and do not provide easily recorded and dependable forensic evidence. Also, there is no control over the digital signing process, and software cryptographic processing cannot be observed, much less understood, by end users. Thus, commercial computing systems are not suitable to be held as good evidence in a civil dispute whose resolution depends upon the weighing of the "balance of probabilities" (McCullagh and Caelli, 2000).

5.4. THE ABSENCE OF "ROLES"

There have been many discussions amongst researchers on the problem of delegating responsibility and trust (Crispo, 1998; Harbison, 1998). What is not addressed properly is the recognition of roles, departmentalisation of organisations and division of job functions which has existed since Biblical times (The Holy Bible, 1984; Stoner et al., 1997). A job position or role is maintained by

an organisation. A member or employee of the organisation is appointed to fill the role, and the appointed person may change over time. A signature made by the person at a point in time is performed under the authority of the position within the organisation.

Commercial paper documents and contracts normally display the originating organisation's letterhead, the job position of the signer and his or her name. The handwritten signature on the letter serves to authenticate the name (and not the other way around), and the position implies the authorisation accorded by the organisation. The receiver can check if the signer is the correct and authorised organisation member, and check with the state or national business registry to verify the legitimacy of the organisation. Therefore, it is strange to base business to business trust on the verification of a public key certificate of a signer provided by a third party (CA) that does not know anything about an employee's position or organisation's purpose. In normal business these should be accomplished by recourse to the organisation or to a business registry, respectively.

In the normal B2B commerce case, verification of the authority and validity of a document is done with the organisation or department in question on a need-to-know basis, clearly a more efficient and flexible as well as time-honoured practice. A hierarchical, X.509 certificate based PKI attempts to act as a large, distributed Access Control List (ACL) for individual end-user entities. Certificate revocation is meant to be broadcast throughout the PKI, which is difficult to carry out (Davis, 1996). In contrast, in a normal business case, when a person leaves an organisation, centralised information servers revoke the person's authorisation and privileges. This does not require a broadcast to the entire organisation or to those outside it, such as trading partners.

A PKI structured on the CA and X.509 certificate concepts does not and cannot provide an universal signing function for various business and social purposes. Digital signatures that are not tied to a particular context are meaningless (Feigenbaum, 1998). It is highly possible that a certificate verifier (user) only sees the correct verification of an electronic purchase order signed by an Adam Smith of ACME Corporation without realising that Smith is actually a rogue ACME system administrator. This scenario is compounded by the fact that CAs are not concerned about a "certified" signer's authority to sign any particular document.

In the B2B context, an organisation handles and bears the authority of signing, while this authority is then delegated onto designated individuals. Authorisation mechanisms such as Simple Distributed Security Infrastructure (SDSI) (Rivest, 1998), credential certificates (Ellison, 1999) recognise the need for delegation of authority, but they do not recognise the purpose of roles, which are essentially privileges and restrictions of a user, and are prevalent in access control literature.

A person is assigned into a particular role in an organsation, and is authorised by his organisation to sign or delegate executive authority to certain colleagues.

Consequently, public key signing functions need to be integrated into access control systems, as much as employee responsibilities and authority are fitted into roles in a structured corporate hierarchy.

6. NEW PROPOSALS

Corporations are responsible for delegating the responsibilities and executive powers of its personnel. In a similar way, national business registration authorities track the existence of commercial enterprises. Professional organisations, such as medical, accounting and legal councils regulate their respective practitioners. Certification by respective authorities would probably be more trusted and recognised than a CA that issues generic certificates.

6.1. "RELIABLE" CERTIFYING AGENCIES

Evidently, at the moment such authorities are not yet utilised in the digital domain, e.g. Internet domain name registration, etc. It is suggested that they are in a far better position than commercial vendors to provide the social authority desired in commerce and industry.

Across national borders, cross verification between such authorities could be in a "web of trust" structure, where the number of links maintained by each authority in its domain of interest is approximately limited to the number of participating United Nation countries.

The argument is that an existing social authority or entity should see itself as a digital "certification" authority. (This is not the same as a current CA providing X.509 digital certificate services).

Governments would, at a minimum, play a regulatory role to provide trustworthy, verified mechanisms. A governmental department could be created to manage public cryptographic keys, in the same manner that a government does today through issuance of a passport, registration of companies, etc. A national government has a more enduring permanence than corporations, which may be subject to more common dissolution. Such a government agency would aim to provide a critical function in society, as opposed to a CA where profit is its primary purpose.

6.2. DIGITAL SIGNING WITH ROLES

There is a natural gap between the world view of an organisation and its actual internal structure and management. It is obvious that organisations normally run their own business and assign roles to their members to accomplish business or like objectives. Ideally, the use of Role-Based Access Control (RBAC) mechanisms in information systems may be used to control digital signing activities. This indeed may correspond to the "name and position" title structure of a authorising signature on a commercial, paper document.

Employees who are vested in the roles are given a set of keys stored on tamper-resistant hardware such as smart cards that may now be used to act for the company or entity. In the event that an employee is unable to be in the office, for example, due to illness, accident or death, another employee can take over that job function without significantly undermining the operation of the role. Delegation thus becomes a normal part of the B2B e-commerce structure, mirroring usual business practice.

Figure 2 shows the order in which an electronic message is signed by Bob with his own personal key, followed by the role CEO and the company ACME Corp. (where the role and company signing are performed by separate, trusted computers). In the event that Bob is away for a meeting, a delegated manager Alice can sign on Bob's behalf, and she would be potentially responsible for any discrepancies. The activation of role and/or company keys by personnel or machine are left to individual corporate policies.

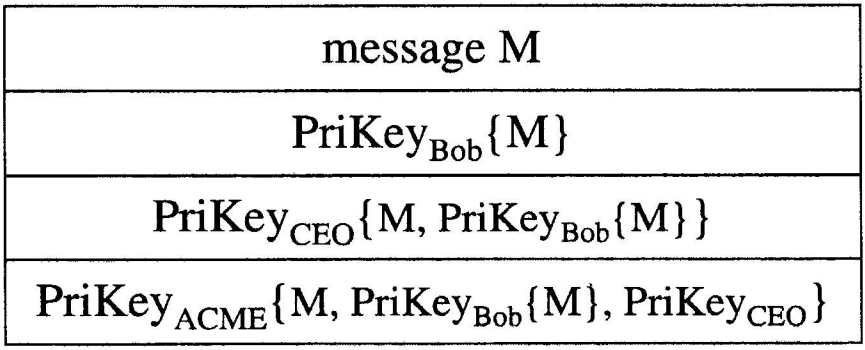

Figure 2 Proposed Digital Signature Hierarchy

Company keys can be certified by a business registry, role keys by the organisation, and individual keys by the organisation's human resources department. Such a scheme mirrors paper practices, and its simplicity makes it easier for laymen to adopt such a electronic parallel. Widespread adoption of this method may encourage the growth of B2B PKI-based electronic commerce.

7. CONCLUSION

This paper presents a simple approach to overcoming excessive dependence on X.509 digital certificate structures for B2B electronic commerce activity. Commerce demands reliable and safe methods, particularly where conflict resolution is needed via mediated negotiation or legal recourse, which complex certificate-based PKI structures have failed to provide.

The solution lies in a combination of technical and organisational structures, as follows:

1 Recognition that complex X.509 digital certificate hierarchies and/or networks do not totally meet the needs for efficient and reliable B2B e-commerce demands,

2 Alternative structures based around simplified directory schemes and "trading partner agreements" and other concepts offer far more efficient and scalable solutions,

3 Directory structures and associated legal agreements provide a better solution to the problem of evidentiary collection and presentation in the case of disputes, particularly where these involve legal proceedings,

4 Far more work is needed on the mirroring in information systems and data networks of the time-honoured practice of involvement of a "notary" or "witness" to an important set of transactions, such as those relevant to the B2B environment as distinct to the business-to-consumer (B2C) situation involving much smaller level transactions.

The crux of the infrastructure issue in B2B electronic commerce is not simply concerned with advanced cryptographic or security techniques. It is about providing electronic services and mechanisms that are at least equivalent to, and hopefully superior to, current social and legal rules deeply embedded in human society.

References

ABA (1996). *Digital Signature Guidelines.* American Bar Association.

Adams, C. and Lloyd, S. (1999). *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations.* Macmillan Technical Publishing, Indianapolis, Indiana.

Anderson, R. J. (1994a). Liability and Computer Security - Nine Principles. In *Proceedings of the Third ESORICS,* volume 875 of *Lecture Notes in Computer Science,* pages 231–245. Springer-Verlag.

Anderson, R. J. (1994b). Why Cryptosystems Fail. *Communications of the ACM,* 37:32–40.

Berkovits, S., Chokhani, S., Furlong, J. A., Geiter, J. A., and Guild, J. C. (1994). Public key infrastructure study: Final report. Technical report, Mitre Corporation.

Biddle, C. B. (1996). Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure. Unpublished but submitted to San Diego Law Review Vol. 33.

Crispo, B. (1998). Delegation of Responsibilities (Transcript of Discussion). In *6th International Workshop on Security Protocols,* volume 1318 of *Lecture Notes in Computer Science,* pages 124–130. Springer-Verlag.

Davis, D. (1996). Compliance Defects in Public Key Cryptography. In *Proceedings 6th USENIXSecurity Symposium,* pages 171–178, San Jose, California. Usenix Association.

Dierstein, R. (1990). The Concept of Secure Information Processing Systems and Their Basic Functions. In *Proceedings of 6th IFIP/Sec'90,* pages 133–149, Helsinki, Finland. North Holland.

Diffie, W. and Hellman, M. (1976a). Multiuser Cryptographic Techniques. In *Proceedings of AFIPS National Computer Conference,* pages 109–112. AFIPS.

Diffie, W. and Hellman, M. (1976b). New Directions in Cryptography. *IEEE Transactions on Information Theory,* IT-22(6):644–654.

E-Sign Act (2000). Electronic Signatures in Global and National Commerce Act. Second session of the 106th Congress of the United States of America on 24 January 2000.

Ellison, C. (1999). SPKI Requirements. RFC 2692.

Ellison, C. and Schneier, B. (2000). Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure. *Computer Security Journal,* 16(1):1–7.

Feigenbaum, J. (1998). Towards an Infrastructure for Authorization. In *3rd Usenix Workshop on Electronic Commerce,* pages 15–19, Boston, Massachusetts. USENIX Association.

Harbison, W. S. (1998). Delegating Trust (Transcript of Discussion). In *6th International Workshop on Security Protocols,* volume 1318 of *Lecture Notes in Computer Science,* pages 108–117. Springer-Verlag.

Jueneman, R. R. and Robertson, Jr., R. J. (1998). Biometrics and Digital Signatures in Electronic Commerce. *Jurimetrics Journal of Law, Science and Technology,* 38:427–457.

Kimberley, P. (1991). *Electronic Data Interchange : A Review of the Current Status of Electronic Data Interchange Throughout the World and an Introduction to the Services.* McGraw-Hill.

Kohnfelder, L. M. (1978). Towards a Practical Public-key Cryptosystem. Bachelor's thesis, Department of Electrical Engineering, MIT.

Landrock, P. (1999). Challenging the conventional view of PKI - will it really work? In *Proceedings of 16th World Conference on Computer Security, Audit & Control,* pages 406–424, Westminster, London. Elsevier.

McCullagh, A. and Caelli, W. J. (2000). Non-Repudiation in the Digital Environment. *First Monday,* 5(8).

McCullagh, A., Little, P., and Caelli, W. (1998). Electronic Signatures: Understand the Past to develop the Future. *University of NSW Law Journal,* 21(2).

Nygh, P. E. and Butt, P., editors (1997). *Butterworths Australian Legal Dictionary.* Butterworths, Sydney.

Rivest, R. L. (1998). Can We Eliminate Certificate Revocation Lists? In *Proceedings of Financial Cryptography '98,* pages 178–183, Berlin. Springer-Verlag.

Sneddon, M. (1998). Legislating to Facilitate Electronic Signatures and Records: Exceptions, Standards and the Impact on the Statute Book. *University of NSW Law Journal,* 21(2).

Stoner, J. A. F., Yetton, P. W., Criag, J. F., and Johnston, K. D. (1997). *Management.* Prentice-Hall, Sydney, Australia, second edition.

The Holy Bible (1984). *The Holy Bible.* International Bible Society, East Brunswick, New Jersey, New International Version edition. Exodus Ch. 18 v. 13–23.

Thompson, K. (1984). Reflections on Trusting Trust. *Communications of the ACM,* 27(8):761–763.

Verisign Inc. (2000). Verisign OnSite White Paper. Available at `http://www.verisign.com/onsite/white paper.html`.

Acknowledgments

The authors wish to thank their colleagues in the Information Research Security Centre, Queensland University of Technology for the lively discussions an this topic.

Kok Ming Ang graduated with a Honours degree in the Information Security Research Centre (ISRC) at the Queensland University of Technology, Brisbane, Queensland, Australia.

William J. Caelli is the Head of the School of Data Communications and a Member of the Information Security Research Centre (ISRC) at the Queensland University of Technology, Brisbane, Queensland, Australia. Prof Caelli is the research supervisor for Mr Ang.