PKI implementation issues in B2B e-commerce

Pita Jarupunphol and Chris J. Mitchell
Information Security Group, Royal Holloway, University of London

About the authors

Pita Jarupunphol (B.B.A. (Dhurakijpundit) MCOM (Wollongong)) completed a B.B.A. in Business Computing from Dhurakijpundit University, Bangkok, Thailand (1997) and an MCOM in Information Systems from the University of Wollongong, Australia (1999). Work experience includes Computer Staff, Wahrin Machinery, Thailand (1997-1998), Computer Lab Supervisor, Illarwarra Technology Corporation, Australia (1998-1999), and Lecturer at the Department of Business Computing, Dhurakijpundit University, Thailand (1999-2000). He received a scholarship from the Rajabhat Phuket Institute for an MPhil/PhD in Information Security at Royal Holloway, University of London. His research interests include secure e-commerce applications, end-user risk perceptions in e-commerce, and public key infrastructure (PKI).

Professor Chris Mitchell (BSc PhD (London) CEng CMath FBCS FIEE FIMA) received his B.Sc. (1975) and Ph.D. (1979) degrees in Mathematics from Westfield College, London University. Prior to his appointment in 1990 as Professor of Computer Science at Royal Holloway, University of London, he was a Project Manager in the Networks and Communications Laboratory of Hewlett-Packard Laboratories in Bristol, which he joined in 1985. Between 1979 and 1985 he was at Racal-Comsec Ltd. (Salisbury, UK), latterly as Chief Mathematician. He has played an active role in a number of international collaborative projects, including the ongoing Mobile VCE Core 2 and Core 3 programmes, three current EU 5th Framework projects (SHAMAN and PAMPAS on mobile security, and USB_Crypt dealing with novel security tokens), a recently completed EU 5th framework project combining smart cards and biometrics (Finger_Card), and two EU ACTS projects on security for third generation mobile telecommunications systems (USECA and ASPeCT). He is currently convenor of Technical Panel 2 of BSI IST/33, dealing with security mechanisms and providing input to ISO/IEC JTC1/SC27 on which he has served as a UK Expert since 1992. He has edited six international security standards and published well over 100 research papers. He is academic editor of Computer and Communications Security Abstracts, and a member of the Editorial Advisory Board for the journals of the London Mathematical Society. He continues to act as a consultant on a variety of topics in information security.

Mailing address: Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK; Phone: +44 (0)1784 443423; Fax: +44 (0)1784 430766; E-mail: {P.Jarupunphol, C.Mitchell}@rhul.ac.uk.

continued on page 2

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

Descriptors

electronic Commerce (e-commerce), public key infrastructure (PKI), public key cryptography (PKC), digital certificate, digital signature, interoperability.

Reference to this paper should be made as follows:
Jarupunphol, P. & Mitchell C. (2003). PKI Implementation Issues in B2B E-Commerce. In U.E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings (ISBN: 87-987271-2-5) 14 pages. Copenhagen: EICAR.

PKI implementation issues in B2B e-commerce

Abstract

The security of sensitive information transmitted and stored during e-commerce transactions is clearly an overriding issue of concern to organisations and individuals. Not only is there a need for the protection of the confidentiality and integrity of sensitive information, but verification of the identity of a communicating party is often also necessary. Public Key Infrastructures or PKIs have long been promoted as an important part of a solution to these concerns, since they support the wide scale use of public key cryptography to fulfil end-user security requirements. Although PKIs involving a single CA are effective when implemented within a well-defined population, the implementation of PKIs across multiple domains and hence involving multiple CAs, e.g. as required for e-commerce, has encountered serious problems. The intention of this paper is to discuss the main reasons for the PKI implementation issues in B2B e-commerce and to propose potential solutions.

Background

As has been widely discussed in the literature (see, for example, (Menezes, van Oorschot, & Vanstone, 1996)) public key cryptography (PKC) supports a variety of practically valuable cryptographic operations including encryption, digital signature and entity authentication. The use of PKC requires all parties to have their own key pair, made up of a public key (usually widely distributed) and a private key (known only to its owner). Verifying a digital signature, or sending encrypted data, requires possession of a trusted copy of the public key of the creator of the signature or the recipient of the encrypted data.

The trusted distribution of public keys is the primary purpose of a PKI. A PKI usually contains of one or more Trusted Third Parties (TTPs) called Certification Authorities (CAs). A CA creates public key certificates, where a certificate is the concatenation of the name of an entity (the subject of the certificate) with the public key of that entity (and other data), all signed using a private digital signature key owned by the CA. If a third party possesses the CA's public key (often called a 'root key') then this can be used to verify the certificate and hence obtain a trusted copy of the subject's public key. In general a PKI consists of a set of CAs, the set of certificates they have generated, the policy under which the certificates were issued, and various other parties (and protocol interfaces) involved in supporting the generation, management and distribution of public key certificates.

Overview of PKI aspects in e-commerce

PKI is the subject of standardisation by a number of bodies, including the IETF, ITU-T and ISO/IEC – for further details see, for example, (Mitchell, 2000). We now discuss how PKI can be used to support security mechanisms of importance to Internet e-commerce.

In order to support a PKI service, a trusted third party (TTP), who plays the role of a CA, is required. Although there can be various types of TTP,

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

including trade platforms, public CAs, and corporate CAs (Helmich, 2000), we focus here on trade platforms that support B2B e-commerce security.

PKI services in e-commerce

In e-commerce, security of sensitive information and reliable identification of trading partners are very important factors. Confidentiality, integrity, authentication, and non-repudiation are all security requirements. These requirements can be supported by a variety of different key management architectures, e.g. secret-key based Key Management Centres (KMCs), as well as by PKIs. Some significant benefits of PKIs over secret-key based key management architectures, such as those based on KMCs, are as follows.

- In a PKI-based system, there is typically much less on-line interaction between clients and key management authorities (such as CAs) than there is in a secret key based system, where typically the KMC will be involved in setting up every session key.
- Unlike in secret-key based key management systems, it is unnecessary for end-users to store a number of keys in order to exchange secured messages with a specific recipient. End-users can either transfer the necessary public key certificates between themselves, or can obtain the necessary certificates dynamically from a certificate repository.
- In secret-key based systems, it is difficult to initiate a key exchange between parties from different organisations who have not previously communicated (Adams and Lloyd, 1999). Supporting secure communications between such parties using a PKI, whilst still non-trivial, is potentially much easier to manage. The two organisations concerned must first agree how their PKIs can interact, and then they must generate a pair of 'cross-certificates', i.e. public key certificates generated by one CA for the public key of another CA – see, for example, Section 13.6.2 of (Menezes et al., 1996). In many cases this will be sufficient to enable all pairs of parties covered by the respective organisations' PKIs to set up secure communications.
- The use of public key cryptography, as supported by a PKI, and in particular the use of digital signatures, enables non-repudiation services to be readily supported. Such services enable one party to prevent another party denying having taken a particular action, e.g. sending a message. Such services are very difficult to support in a secret key based architecture.

PKI implementation requirements

We next consider the steps that need to be taken by any organisation wishing to deploy a PKI. Note that we focus our attention here on organisations wishing to use a PKI to support the provision of security services for B2B e-commerce, although many of the remarks apply more generally.

Stage 1: Gather information Potential PKI end-users must gather information about PKIs from either internal or external sources. This includes

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

information regarding the benefits of PKI implementation, the cost of PKI implementation, methods for providing a PKI, i.e. internal or external provision (outsourcing), PKI provider selection (in the case of outsourcing), i.e. which is the most cost-effective and trustworthy provider, and (in the case of internal provision) PKI software vendor selection.

Stage 2: Make decision PKI end-users must make a decision as to whether or not to adopt a PKI based on the information gathered in the previous stage. If a decision to adopt a PKI-based solution has been made, the next step is to choose the method to provide the PKI.

Stage 3: Choose PKI vendors There are advantages and disadvantages of both internal and external provision of a PKI. Using internal experts to set up a PKI may not always be feasible, e.g. because of a lack of expertise within the organisation. However, relying on PKI outsourcing also holds potential pitfalls and risks, e.g. breaches of confidentiality and breach of a company's obligations under data protection law (Fenn, Shooter, & Allan, 2002).

Stage 4: Prepare infrastructure The infrastructure required to support a PKI is very complex, involving a variety of activities including CA policy and procedure establishment, CA initialisation, CA public key distribution, end-user certificate generation and distribution (including user registration), revocation mechanism establishment, and (perhaps most important of all) user education.

Stage 5: Implement PKI Once end-users have generated or been given their key pair(s), and have been provided with a certificate for their own public key(s), they can readily establish secure communications with other end-users by validating and exchanging certificates as necessary. However, private keys can be compromised and/or revoked for other reasons (e.g. because an individual changes their job). Thus, before using a public key it is typically necessary to check whether or not it has been revoked. This typically involves either checking a digitally signed Certificate Revocation List (CRL) or making on-line checks with a trusted third party server which maintains accurate revocation information. When using certificates across organisation boundaries, this revocation checking can become rather complex.

PKI interoperability issues in e-commerce

The most basic PKI architecture is one that contains a single CA that provides the PKI services, including certificate generation and the provision of certificate status information, for all PKI end-users. Using and managing a PKI seems to be relatively straightforward within a ‘controllable environment’, such as a single organisation containing several subordinate departments. In B2B e-commerce, however, it is necessary to utilise a more complex PKI architecture involving multiple CAs, since it involves trading via digital means between partners who will typically each have their own CA.

Apart from security services, there are other associated factors to consider, such as real-time service, time of goods delivery, etc. To fulfil consumer

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

requirements, it is crucial for an e-commerce organisation to have efficient supply chain management (Lee and Whan, 2001). Typical requirements for an e-commerce trading company are as follows.

- A company must be able to communicate with its suppliers and customers quickly and securely in order to operate at maximum efficiency and to provide a timely service to its consumers.
- A company must be able to co-operate with other e-commerce companies in order to share and exchange information.

In order to meet these requirements, there is a need for e-commerce organisations to be able to establish secure communications links. For example, for real-time value chain management, someone working in a factory for company A may need to communicate with someone in the accounts department of company B as well as someone in the procurement department of company C. It is natural to attempt to re-use existing PKIs, already established within companies for internal security, as the basis for secure inter-company communications. Indeed, if this were to be possible, then the benefits would be potentially great.

However it appears to be very difficult to achieve the necessary level of inter-operation between two different PKIs. Fundamentally, a PKI is normally established with a set of rules and understandings about the meaning and use of public key certificates. This set of rules may be explicit as a Certificate Policy and/or Certification Practice Statement, or it may be implicit. The problem with inter-working between PKIs is that these sets of rules and understandings are almost inevitably different, which means that interpreting a certificate issued as part of a different PKI becomes very problematic.

As a consequence, interoperability has become a serious issue impeding the growth of PKI in the e-commerce arena. Although a number of efforts have already been made to try and facilitate PKI interoperability (see, for example, PKI forum, 2001), it remains a major problem. We now consider in somewhat more detail some of the reasons underlying these interoperability problems (similar work is being carried out by other parties, such as the Fiducia Project http://csrc.lse.ac.uk).

Different X.509 extensions

Typically, PKIs in different organisations will have been procured from different vendors. Hence, although all the public key certificates may conform to the current version of the X.509 recommendation (ITU-T, 2000), the two vendors will have chosen different options and will be using different sets of critical extensions, where a critical extension is a field in a certificate which must be processed by the verifier of the certificate. This arises because of the unbounded flexibility offered by the X.509 extensions. Furthermore, some of these extensions may be proprietary which, if they are critical, means that processing certificates may be impossible. This is supported by (Helmich, 2000), who states that certificates from Entrust may be incompatible with certificates from other vendors, such as Baltimore.

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

Different policies for issued certificates

As briefly mentioned above, a Certificate Policy (CP) and a Certification Practice Statement (CPS) should be established in order to implement a PKI effectively. Each company will potentially have a different CP and CPS, since they would normally be drawn up to reflect the particular practices and requirements of that company. Hence, there will clearly be issues in interpreting the meaning and validity of certificates generated by a different organisation.

Different obligations on certificate subjects

Public key cryptography relies on the holder of a private key looking after it carefully, and preventing its disclosure to any other party, except as authorised by the CP in force. The CP will typically place obligations on the certificate subject, i.e. the holder of the private key, to maintain the secrecy of his/her private key. However, different policies may place different obligations on private key holders. Consequently, another issue that will vary between PKI implementations relates to the obligations on certificate subjects, in particular with regard to maintaining the secrecy of their private keys.

Different liability protection

A public key certificate, as issued by a CA, can be seen as a guarantee by that CA that a particular public key belongs to a specified entity. Moreover, while the certificate's expiry date has not passed and it has not been revoked by the CA, e.g. through a Certification Revocation List (CRL), there is an additional guarantee that the private key has not been compromised. Of course, the meaning of this 'guarantee' will vary depending on the CP and CPS.

Nonetheless, for the PKI to have much value, particularly for inter-company communications, one might expect the CA to take on some liability for the correctness of its guarantees. That is, it might be expected to offer some kind of compensation in the event that an individual uses a certificate only to subsequently discover that it is not valid. Problems will immediately arise in this context because different organisations will provide different levels of liability transfer. This is potentially a very serious obstacle to PKI interoperation.

Different features in PKI applications

A PKI-enabled application is software that supports public key cryptographic mechanisms and accesses 'the key/certificate life cycle-management functions' (Adams and Lloyd, 1999: 269). Different applications will have varying requirements on the nature of the underlying PKI, and different organisations will use different sets of applications. This may well mean that a PKI-enabled application in one organisation is simply unable to use a

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

certificate generated by a different organisation, irrespective of concerns about issues such as certificate meaning and CA liability.

Different certificate storage and retrieval standards

After they have been generated by a CA, public key certificates typically need to be available on-line for anyone who may need them. There are two different standardised means for certificate storage and retrieval, namely the ITU-T X.500 recommendations (ITU-T, 2000) and use of IETF LDAP (Boeyen, Howes, & Richard, 1999). Whilst LDAP is widely used, some systems are built around X.500, which can cause serious interoperability issues.

Different PKI knowledge among organisational staff

Adams and Lloyd (1999) claim that there is a shortage of staff who have a sophisticated understanding of PKI technology, probably because of the very recent rapid growth in availability and use of PKI-based solutions. Knowledge regarding PKI is required not only for low-level staff, but also for high-level staff who are responsible for developing the CP. This need for understanding of the technology, when combined with the lack of staff with the required knowledge, itself contributes to difficulties in enabling interoperation between PKIs.

Models for PKI interoperation

A number of models exist for defining relationships between CAs. The choice of model itself affects the interoperability issue. The three models most commonly discussed are the hierarchical model, the peer-to-peer (or 'mesh') model, and the bridge model (see also figure 1). We now briefly introduce each of these models, and consider their advantages and disadvantages within the context of B2B e-commerce.

Before proceeding note that the models essentially define which pairs of CAs establish a direct relationship. This inter-CA relationship will involve the trusted exchange of public keys, and the generation of a pair of 'special' public key certificates, called 'cross-certificates'. That is, if CAs A and B establish a relationship, then A will sign a public key certificate for B, and vice versa. If a 'client' of A, i.e. an entity within the scope of the PKI to which A belongs, wishes to verify a public key certificate signed by B, then the client can first verify the appropriate cross-certificate to validate B's public key, which will then enable the client to verify B's signature on the target public key certificate. This notion of cross-certification can be extended to a certification chain, where a series of cross-certificates 'connecting' the required pair of CAs is validated.

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

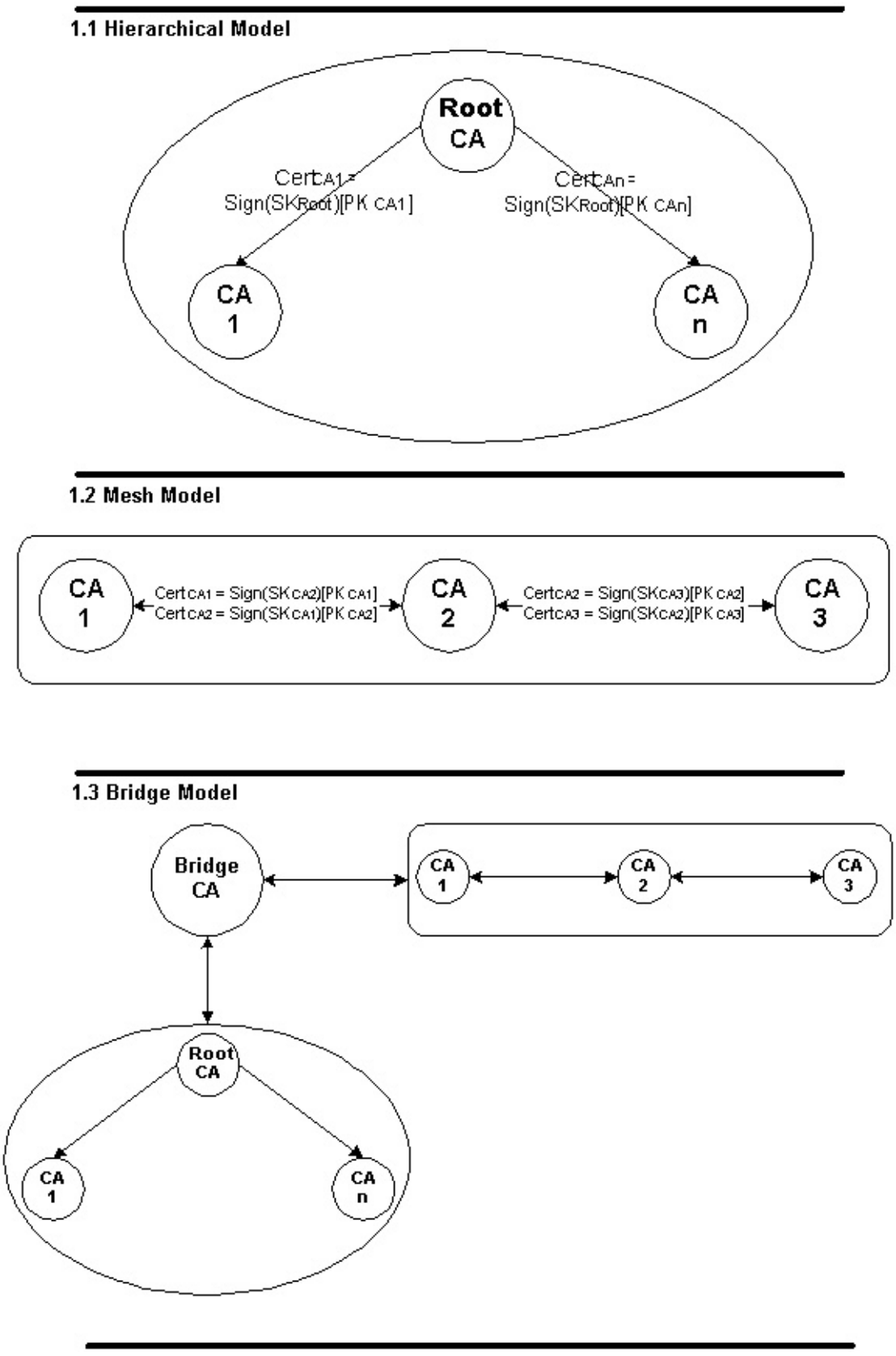

Figure 1. PKI interoperation models.

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

Hierarchical Model

In the hierarchical model, all the CAs are arranged in a strict hierarchy, with a defined 'root CA' which is above every other CA in this hierarchy. Every pair of CAs will then possess a common CA superior to them both in the hierarchy. This means that an end user can easily determine a unique certificate chain which will enable him to verify any other entity's public key.

Whilst this sounds simple and appealing, it is not a model which readily maps to most real world situations. The CA hierarchy needs to correspond to a matching trust hierarchy, or the solution will be almost impossible to operate. However, corporate entities operating CAs which need to interoperate to support B2B e-commerce will typically not belong to a natural trust hierarchy, and so the solution will simply not apply. Moreover, even if a hierarchy of CAs could be effectively operated, this puts an enormous load of trust on a single point of failure, namely the 'root CA'. (However, this concentration of trust may be inevitable, as it also holds for a much more useable model, namely the bridge model, which we consider below).

Peer-to-Peer (Mesh) Model

The peer-to-peer model allows any pair of CAs to establish a cross-certification relationship. This corresponds much more closely to business reality, and will probably work well for small communities of organisations (small numbers of CAs) where every pair of CAs can set up a relationship. This will then mean that it will only ever be necessary for an end-user to verify a single cross-certificate.

Unfortunately, such a solution will clearly not scale well to a large number of CAs, as we might expect to exist in a complex multi-national world of e-trading. Of course, it can be argued that it will not be necessary for every pair of CAs to establish a relationship, and certificate chains can be 'discovered' on an ad hoc basis. There are two major problems with such an approach. First, it places a potentially unacceptable load on the end-user. Second, the likelihood of any effective transfer of trust, as required for PKI interoperation to work, being achieved using a chain constructed in an ad hoc way is very small.

Bridge Model

The bridge model is, to some extent at least, a compromise between the previous two models. In this model, one or more 'bridge' CAs exist, which set up relationships with all other CAs. In this way a certificate chain consisting of a pair of cross-certificates will always be sufficient to enable an end-user to verify another user's public key certificate.

This model requires far fewer cross-certificates to be created then the basic peer-to-peer model, and yet still enables the end-user to readily establish a short and well-defined certificate chain. The only problem that remains is that of identifying entities suitable to provide and operate the bridge CAs. Such

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

organisations must have a well-defined trust relationship with every other CA. One possible candidate for operating a bridge CA might be a national government – as in the US federal bridge (Draft 101500, 2000). Indeed, as reported in the draft, positive results from the operation of this Federal Bridge CA (FBCA) have been achieved. However, such a solution is unlikely to solve international interoperation issues. Hence other candidates are required.

Addressing PKI interoperability issues

We now consider how to address some of the PKI interoperability issues raised in the first section. We provide a series of possible practical steps which may help to reduce these interoperability issues.

Profile PKI standards Well-defined profiles for PKI standards must be established, strictly limiting the options for the structure of public key certificates, and in particular limiting the use of the extension fields. These profiles must be carefully designed to both allow individual organisations the flexibility they need within their individual PKIs, and to provide for seamless interworking between organisations.

Use and develop the bridge model The bridge model, as discussed in Section 6.3, has considerable potential to enable interworking between PKIs in a B2B e-commerce environment. This has been supported by the results of the FBCA trials (Draft 101500, 2000). Further research into, and practical trials of, such bridge CAs is/are urgently required, in order to establish more precisely the degree to which such bridge CAs can successfully deal with the day to day interoperation requirements arising from B2B e-commerce.

Educate staff regarding PKI technology In order to operate a PKI effectively, staff at all levels must be equipped with the necessary knowledge about PKI technology. This will enable the organisation management to set appropriate policies and practice statements, and also enable those operating the PKI to do it in a secure and effective way. As with all aspects of security, all staff need to be made aware of the importance of operating and using a PKI in accordance with the policy and rules.

Role of industry associations and trade bodies To make the bridge model work requires an appropriate organisation to operate a bridge CA. For such a solution to work also requires general agreement about the meaning and management of public key certificates, i.e. the establishment of shared ‘baseline’ CPs and CPSs. The question then naturally arises as to who operates the bridge CA and who establishes the baseline CP and CPS. Whilst standards bodies and international treaties offer a possible solution, such approaches tend to take many years to come to fruition. It may be much easier to achieve a timely solution through voluntary trade associations and industry organisations. Given that entire industries will have very major business incentives to find and establish speedy solutions, looking to bodies funded by the industry itself to generate the necessary solutions seems a reasonable approach.

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

New models for establishing liability transfer One issue raised above relates to the difficulties in establishing the level of liability protection offered by a different CA. In fact this issue is a problem affecting almost every user of PKI technology. It is often difficult for a CA to find ways of generating sufficient revenue to be able to offer significant liability protection. One way in which this general problem could be solved is through novel means of generating revenue for liability transfer. One possibility which merits further research is through the use of on-line certificate status servers. Such servers could make a charge for their service, and at the same time offer a 'one off' liability protection for this invocation of their service. The certificate status server would essentially be offering a kind of insurance, with the fee being a premium for this insurance.

Certificate translation services In the short to medium term, it is unlikely that all organisations within an industry sector will be able to agree and implement a single tightly-defined certificate profile. Hence, for the next few years problems with the inability to process certificates generated by different PKIs will continue. One possible means to address this problem is through the use of a certificate translation service (Borselius and Mitchell, 2000). Such a service would take a public key certificate as input, verify it, and then output a new certificate in a form processable by the requester. This new certificate would, of course, be signed by the translation server rather than the original CA, and hence the translation server would need to be trusted. Indeed, such a server could be integrated with the bridge CA and/or with a certificate status server, thereby reducing the number of required trusted nodes. Such an approach would remove the need for every end-user to be able to process every other user's certificates, and would simply require one server to be equipped with the means to understand every certificate type.

Government support National governments (and supranational bodies such as the European Commission) can also play an important role in supporting the measures necessary to achieve PKI interoperation. For interactions occurring only at a national level, government-backed bridge CAs (such as the FBCA) will be appropriate. Governments can also provide guidance on the use and contents of certificate profiles, e.g. by promoting standards development or by directly supporting the necessary research and development.

Establish connections among Bridge CAs Although the FBCA can establish trust relationships among different PKI platforms, it is of limited value if two organisations would like to trade internationally. However, one possible solution might be to first establish national bridge CAs, and then establish connections with other national bridge CAs using the PKI mesh model. In this case, the issue of the large number of CAs may not be such a serious issue, since the number of countries is far less than the number of companies who may wish to conduct B2B e-commerce.

Conclusions and remarks

The use of PKI to underpin B2B e-commerce security has many advantages, not least since many organisations have already implemented PKI to support

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

internal security functions. However, as we have discussed in this paper, there are a number of serious interoperability issues limiting the use of a PKI across organisation boundaries. Removing these obstacles to PKI interoperation is critical for the future health of B2B e-commerce. We have proposed a series of practical steps which can be used to try and address the major PKI interoperability problems, thereby promoting the future use of PKI across corporate domain boundaries.

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

References

Draft 101500 (2000). Report of Federal Bridge Certification Authority Initiative and Demonstration.

ITU-T (2000). Recommendation X.509 (03/00) – Information technology – Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks, March.

PKI forum (2001). PKI Interoperability Framework, March.

Adams, C. and Lloyd, S. (1999). Understanding Public-Key Infrastructure. Indianapolis: Macmillan.

Boeyen, S., Howes, T., and Richard, P. (1999). Internet X.509 Public Key Infrastructure Operational Protocols – LDAPv2, April. Available: http://www.ietf.org/rfc/rfc2559.txt.

Borselius, N. and Mitchell, C. J. (2000). Certificate translation. In Proceedings of NORDSEC 2000 – 5th Nordic Workshop on Secure IT Systems, 289–300, October.

Fenn, C., Shooter, R., and Allan, K. (2002). IT security outsourcing: How safe is your IT security?. Computer Law & Security Report, 18(2): 109–111.

Helmich, P. (2000). Public key infrastructures: A panacea solution?. Network Security, 2000(5): 8–11.

Lee, H. L. and Whan, S. (2001). E-business and supply chain integration. Stanford Global Supply Chain Management Forum, 1–20, November. Available: http://www.stanford.edu/group/scforum/Welcome/EB_SCI.pdf.

Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A. (1996). Handbook of Applied Cryptography. Boca Raton: CRC Press.

Mitchell, C. J. (2000). PKI standards. Information Security Technical Report, 5(4): 17–32, November.

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS