

Position Statement on PKI of the Australian Security Industry

*Prepared by Stephen Wilson
Australian IT Security Forum (AITSF)
Version 3.0, November 2003*

The Australian IT Security Forum has reached a position on the best use of Public Key Infrastructure. Our vision has been developed through extensive dialogue with users and with government. The position is deeply informed by practical experience of some of the world's largest and most effective PKI rollouts. We present here the major implications of this experience for systems integration, PKI regulation and cross border interoperability.

The overwhelming experience of PKI in practice is that it delivers most value when used for automating paperless routine transactions between parties who have an existing business relationship. In the best PKI applications, parties tend to deal with one another in a well defined formal context. They tend to operate under existing terms and conditions, with contracted or legislated liability arrangements. There is usually a recognised authority over the domain of the transactions, which can take responsibility for registered digital certificate holders. Current examples include e-health, customs, taxation reporting and business banking. It is likely that PKI will be taken up similarly in the near future for higher education, electronic conveyancing and drivers licensing. We can describe this model as *Scheme-based PKI*.

Scheme-based PKI means that we should expect the deployment of multiple digital certificates in various forms, tightly coupled with (or embedded in) specific types of applications. Different digital certificates would be issued and used under specific conditions; registration processes can be streamlined for different user communities; subscriber agreements can be folded into existing user agreements.

The idea of multiple certificates was once alarming, but when embedded invisibly in convenient forms such as smartcards, they need not be any harder to use than conventional plastic cards. There is increasing awareness from the perspectives of privacy, usability and commerciality, that a single identity would not be useful in any case. The reality of physically different cards for banking, drivers licence, health insurance, professional memberships and building access is here to stay – irrespective of whether the cards are based on magnetic stripes or PKI.

The main governance and regulatory implications of scheme-based PKI are as follows:

- We should maintain high standards of cryptographic, physical, logical and operational security over backend Certificate Authorities, as typified for example by Gatekeeper.
- We should take a light touch with front-end registration processes, in particular allowing ID-proofing rules to be set by each PKI scheme, fit for the intended purpose of their certificates, rather than seeking to standardise

general purpose evidence of identity rules as if all certificates were equivalent.

- We do not in general need complicated cross-certification or Bridge CA systems which basically seek to establish the equivalence of digital certificates, because the business requirement of relying parties is simply to be able to tell automatically if a certificate is fit for purpose in the users' application domain.
- We do not need major government involvement in the operation or accreditation of PKI schemes. Instead, a governance model akin to the AISEP (Australasian Information Security Evaluation Programme, for conducting Common Criteria assessment) would be most effective, providing trust in the system, a contestable pool of sanctioned assessors, well-defined liability arrangements, and ready pathways to international recognition.

PKI Interoperability through scheme-based PKI

*Prepared by Stephen Wilson
Australian IT Security Forum
Version 3.0, November 2003*

Introduction

First generation PKI has received a fair amount of criticism. Perceived problems with PKI have included intrusive personal identity checks, complex legal arrangements, a lack of good applications, and poor user interfaces. Early PKI applications forced users to look at digital certificates and key management in great detail. The applications required users to read and understand long Certification Practice Statements (CPSs) and required intensive training.

Early PKI applications treated digital certificates like general purpose electronic passports. Most people have generally assumed that a single digital certificate could support a wide range of applications. In this context, the main goal of PKI “interoperability” has usually been for a general purpose digital certificate issued in one jurisdiction to be relied upon without restriction in another jurisdiction. This type of interoperability has been very difficult to achieve because of international differences in identification standards and legal liability provisions.

This paper shows how it is better to treat digital certificates as electronic “business cards”. Instead of representing the personal identity of the holder, digital certificates can represent specific business credentials or professional qualifications. In “scheme based” PKI, different digital certificates are presented for different types of application. The PKI interoperability problem is greatly simplified, because existing business rules in each scheme usually cover identification standards and legal liability.

The problem with first generation PKI

First generation PKI was actually an attempt to create an all-purpose electronic identity. At first it was commonly assumed that we would all need a one-size-fits-all “digital passport” to do e-commerce. Many people falsely believed a single digital certificate would be like a driver's licence and could be used for all-purpose identification over the Internet.

But professionals and business people never use a single identity. Serious business transactions are never conducted between strangers. Instead, serious business transactions are based on professional qualifications or memberships. You use different types of qualifications (or “virtual identities”) in different types of relationships and transactions. The old model of general purpose PKI resulted in much of the overhead (complicated legal arrangements, personal identity checks and poor usability).

Application-specific PKI

PKI has the great benefits of automatic paperless processing, reduced legal risk, and lower cost of dispute resolution. We can obtain these benefits in high value, specialist applications, where digital certificates are application-specific, and are linked to qualifications rather than personal identity.

With application-specific PKI, we can implement new e-commerce architectures and business processes that remove almost all of the first generation overheads.

Public Key Cryptography is admittedly complicated. But traditional authentication technology, such as magnetic stripe card technology, is also complicated. To make these technologies easy to use, we embed them into applications and systems, such as cards. We can issue PKI-enabled smartcards to professionals and business people under existing terms and conditions. Application software can be written so that digital certificate functions are automated and seamless.

Therefore PKI can be as easy to use as any other conventional plastic card. By embedding PKI into smartcard applications, we do not need complex documents, complex legal arrangements, or intensive technical training.

Contemporary PKI

The 'killer applications' for PKI all involve transactions with specific contexts, application software and user qualifications. Examples include tax returns, customs reporting, online healthcare, electronic property conveyancing, superannuation (pension funds) administration and so on. In these cases, users may not know each other personally, but they recognise each other's qualifications. In fact, users should refuse to transact with people unless they are properly qualified. Professional qualifications and memberships are more important than personal identity in business-to-business transactions.

Therefore, contemporary PKI almost always involves specific "communities of interest". All users have a prior business relationship of some sort; often, users will be members of certain associations. They will usually use special transaction software with additional layers of security and access controls.

Electronic business cards are more useful than electronic passports

Digital certificates are much more useful when implemented as application-specific "electronic business cards", rather than as one-size-fits-all electronic passports. We should allow for several electronic business cards, each dedicated to a different type of transaction community, and each with special conditions for different e-business processes. Then we can simplify the registration processes, user experience and legal arrangements.

The true benefits of PKI

In truth, many of the supposed benefits of PKI such as “confidentiality” and “non-repudiation” can be obtained from other technologies. But PKI has two unique benefits:

1. PKI is the only security technology that provides certainty of origin and integrity of electronic documents, over long periods of time, where multiple parties are involved.

Digital signatures do not “fade” with time or with copying. The quality and legal reliability of archived digital signatures remains the same over many years. And if a digitally signed message goes from one person to many others, everyone still receives an identical, verifiable signature code authenticating the original message.

Electronic evidence of the origin and integrity of a message can be provided by means other than a digital signature, such as audit logs. However, the total cost of traditional security technologies is far higher than the cost of PKI. The quality of audit logs is highly variable. It is costly to produce legal evidence from audit logs, especially after long periods of time have elapsed, or if the original transaction has been copied from one machine to another many times.

On the other hand, digital signatures make it much simpler to re-wind transactions (that is, investigate exactly what happened in the past in a complicated transaction in case of suspected fraud). As online fraud steadily rises, businesses are looking to PKI to reduce the cost of investigation, forensics and dispute resolution.

2. Digital signatures and certificates are machine readable, allowing the credentials of the sender to be bound to the message and verified automatically on receipt, enabling totally paperless transacting.

This is an important benefit of digital signatures but it is often overlooked. When processing a digital certificate, the receiver’s software can automatically tell:

- (i) that the message has not been altered since it was originally created
- (ii) that the sender was authorised or qualified to create the transaction
- (iii) that the sender’s qualifications were valid at the time they sent the message
- (iv) that the authority which signed the certificate was also authorised to do so.

Good applications for PKI

Reviewing the two basic benefits of digital signatures helps us to tell which types of e-business applications should be implemented with PKI. Good applications for PKI have the following features:

- Relatively high transaction volume¹
- Fully automatic processing (or “straight-through” processing)
- Multiple receivers
- Significant risk of dispute or need to “re-wind”
- Requirement to retain quality electronic evidence over long periods of time.

A case study in application-specific digital certificates

If digital certificates are constrained to specific applications, then they are much simpler to implement than first generation general purpose PKI.

Consider the American Express Blue credit card, a new PKI-enabled smartcard.

When you sign up for an American Express Blue card, you agree to regular credit card terms and conditions. That is, you agree to keep your PIN secret, not let anyone else use your card, report its loss, and so on. You are not required to read a CPS; you are not required to undertake intensive technical training. The American Express Blue card PKI is completely embedded, so card holders don't even know it is there.

We call this an example of “scheme based” PKI. It is much simpler than first generation general purpose PKI, in terms of ease of use, registration, regulation and legal liability.

This simplification is possible because the American Express Blue digital certificate is tightly constrained. It cannot be used to sign or encrypt generic e-mails, nor to authenticate ordinary SSL connections. In future, only software applications approved by American Express will be able to access the PKI functions embedded in the Blue card. American Express will closely regulate all applications which use its smartcard.

A new interpretation of what digital certificates mean

This experience lets us interpret the meaning of digital certificates in a powerful new way. First generation digital certificates represented personal identity. Now, application-specific digital certificates can represent membership of some defined community, for example a credit card scheme, a professional association, an employer, a government agency, a board of directors, and so on. Each community will have an associated set of e-business applications, with their own special terms & conditions.

¹ Volume is important because the ROI for e-commerce usually relates to reducing paperwork costs.

The purpose of contemporary scheme-based PKI is to automate electronic transactions between parties with specific qualifications. Business-to-business transactions are usually highly structured:

- Sender and receiver only attempt certain types of transactions (for example, a customs office does not usually handle tax returns).
- The sender is authorised to create special transactions due to for example a professional qualification, a government-issued licence, membership of an association, endorsement by their employer, and so on. All receivers recognise these forms of authority. Usually an existing contractual arrangement is in place between sender and receivers.
- Senders and receivers typically use specific forms and/or special purpose application software, adding context and additional layers of security around the transaction.

When PKI is used to automate the online processing of specific transactions between parties with an existing business relationship, then existing legal arrangements should continue to apply. For application specific digital certificates, the question of legal liability is much simpler than in general purpose PKI.

Comparing first generation PKI and contemporary PKI

	First generation PKI	Contemporary PKI
<i>Model</i>	Electronic passport	Electronic business card
<i>Meaning</i>	Personal identity	Qualifications, authorisation, membership etc.
<i>Intended use</i>	General purpose “stranger-to-stranger” e-business	Specific business-to-business transactions between qualified parties with existing relationships
<i>Communities of Interest</i>	Only one: the general public	Many different communities; for example: professions (doctors, pharmacists, lawyers, accountants etc.), business licence holders (customs agents, stock brokers, real estate agents, company secretaries), employees etc.
<i>Implementation</i>	Single general purpose certificate kept separate from software applications	Multiple certificates, specific to software applications and embedded inside the applications
<i>Registration process</i>	Strict face-to-face proof of personal identity	Automatic registration based on existing membership rules and status

Conclusion

The new vision for contemporary scheme-based PKI means the technology is as easy to use as any regular plastic card. Digital certificates are truly not like electronic passports. They are much more powerful when interpreted as electronic business

cards. A digital certificate issued for specific business users can represent any type of professional qualification or membership. Application-specific smartcards can be issued under existing business rules with no additional overhead. Regulators can allow business groups more discretion to set their own registration rules for digital certificates.

We can now embed the complex cryptographic technology into smartcards. All terms & conditions for use of the smartcards can be focused on the application not the technology. Smartcards can be used in exactly the same way as any magnetic stripe card. This approach increases usability, eliminates complex user documents, decreases training burden, and simplifies legal liabilities.