The Importance of PKI Today

Stephen Wilson
Managing Director, Lockstep Consulting Pty Limited, Australia

ABSTRACT

Public Key Infrastructure around the world has had mixed success over the past ten years. Some jurisdictions (like Australia and the USA) have been left largely disillusioned by the hype, while others (like China and Korea) see PKI as indispensable infrastructure for e-business. The typical situation around Asia is that PKI is highly desirable but difficult and/or costly to implement. Regulators tend to be especially confused about their proper role; government PKI licensing programs in places like Singapore, Hong Kong SAR and Australia are not in high demand. This paper presents an update on the PKI business internationally, with a special focus on the role of governments. The paper presents a fresh new "plain speaking" description of the business benefits of PKI, in order to inform government policy reform.

Please note that this paper assumes that the reader is somewhat familiar with PKI concepts. This is not a paper for PKI beginners.

Key words: public key infrastructure, e-business, authentication, security, digital certificates, smartcards, governance

I. INTRODUCTION

Public Key Infrastructure, after being in the "trough of disillusionment" since about 2000, is enjoying a slow but sure recovery. The new interest in PKI thanks to a better understanding of its special properties, and the urgent security needs of new types of e-business. PKI deployments are proceeding rapidly around Asia, mostly influenced by important new models for building "vertical" PKIs. Certain jurisdictions in the region were PKI pioneers throughout the 1990s - including Australia, Hong Kong SAR and Singapore. All countries must examine closely the new PKI experience and be sure to maintain flexible government policies, especially in regard to Certification Authority quality standards and cross border recognition.

II. WHY IS PKI IMPORTANT?

Perhaps no technology better illustrates Gartner Group's famous hype cycle than PKI, with its "peak of inflated expectations", "trough of disillusionment", and now its climb back up the "slope of enlightenment". From the mid to late 1990s, PKI was hyped as being essential to secure e-business, but experience shows that PKI does not have a monopoly on security. E-business is thriving in most places without PKI; for example, legally binding Internet banking1 has been possible in without digital certificates. Indeed, in Australia and the USA, soft certificates were tried and then abandoned by many Internet banks, which found them to be too expensive and too inconvenient compared with the business benefit.

PKI has had its difficulties as a business, in common with most new information technologies. But the unique value of PKI in certain types of online transaction is now widely acknowledged. We have a more sophisticated understanding now of the benefits of PKI. Once it was hoped that digital certificates could produce trust for "stranger-to-stranger"

forms of Internet business. In retrospect, we are not surprised that PKI cannot magically create trust between strangers. So we have updated our understanding of PKI. According to the Australian IT Security Forum,

"... the overwhelming experience of PKI in prac tice is that it delivers most value when used for automating paperless routine transactions between parties who have an existing business relationship" [1].

Therefore PKI take-up is accelerating rapidly around the world, in vertical market places and dedicated applications (see box below).

PKI offers the following unique benefits:

- **digital signatures create persistent, tamper resistant evidence of "who did what to whom"**, which is critical to electronic transactions carrying high legal risks or compliance requirements
- PKI when integrated into smartcards is recognised as **"the only practical solution [to eavesdropping and account hijacking] today"** [2] (see PKI and combating web fraud be low for further details)
- digital certificates can convey **authority information**-like credentials, licences, affiliations **and so on - and digital signatures bind that authority information directly to messages, to decentralise and greatly sim plify transaction processing.**

PKI digital signatures are persistent over both time and "distance". At essentially any future time, a digitally signed transaction can be easily re-validated to prove where it originated. The digital signature code has great longevity. In addition, authority information about the sender can be sealed into their certificate at the time of issue, and this authority information also had

Notable contemporary PKI schemes

- The CableLabs pay TV industry consortium runs a PKI for certificates embedded in millions of settop boxes, with manufacturers run-ning their own special purpose Certificate Authorities.
- Italian companies are required to use online reporting and approved digital certificates for change of registration and annual reports; 2.4million certificates are on issue in Italy andused regularly.
- In Taiwan China, online gaming subscriptions are controlled using the "Play Safe" PKI card, issued so far to 10,000 users and expected to grow to 5 million.
- Taiwan China's National Health Insurance smartcard issued to 22 million citizens is PKI-capable; separately, some 340,000 cards and digital certificates have been issued to Taiwan-ese healthcare professionals.
- The Pan Asia e-commerce Alliance (PAA) oversees nine commercial CAs with 260,000 digital certificates on issue for online trade documentation between Hong Kong SAR, China, Chinese Taipei, Korea, and others.
- Electronic passport chips in the new International Civil Aviation Organisation (ICAO) scheme are digitally signed; the system is said to be upgradeable to include personal certifi-cates for passport holders.
- Johnson & Johnson has issued certificates on USB keys to 100, 000-plus employees for secure e-mail, remote access and ecommerce.
- The credit card companies' new 3D Secure payments protocol is based on digital certificates.
- In Japan, PKI based "residential cards" are issued by prefectures for G2C; numbers are estimated as at least 300,000.
- The authority of Taiwan China offers a personal digital certificate card for G2C transactions,taken up by nearly 1,000,000 citizens so far; smartcard readers are available at convenience stores for US$10 each.
- In Korea, the six largest banks have issued 10 million certificates between them for Internet banking.
- Hong Kong Post has issued 2 million certificates to date, some on diskette, and some on the SMARTICS id card.

great longevity (thanks to the digital signature of the Certificate Authority on the certificate).

The integrity of digitally signed data is not reduced by being copied or forwarded across systems or across borders. In contrast, other authentication technologies rely heavily upon audit logs to prove 'who did what to whom'; therefore forwarding non-PKI transactions from one system to another complicates and dilutes the strength of the audit trail. So PKI is uniquely suited to complex transaction environments, where there might be multiple relying parties, structured data, formal authorisations, and/or long lifetimes.

III. THE RENEWAL IN PKI

Looking more deeply, beyond the surge in applications and schemes listed above, PKI's renewal is most clearly demonstrated by the vitality of the Asia PKI Forum. The APKIF is a coalition of national PKI associations, from China, Hong Kong China, Japan, Korea, Macau China, Singapore, Chinese Taipei, and Vietnam. Observers attend from Thailand and Kazakhstan, and from the international standards bodies OASIS (the Organisation for the Advancement of Structured Information Standards) and ETSI (the European Telecommunications Standards Institute). Malaysia and India are being targeted for membership. The APKIF also corresponds with new regional PKI associations in Mexico, South America and Africa-Mid East.

The APKIF carries out most of its work in four Working Groups - Business Case & Applications, Interoperability, Legal Infrastructure, and Worldwide Collaboration - which all meet quarterly. Its major deliverables are world's best practice. They include in-depth legal analyses of liabilities in cross-border e-commerce and online dispute resolution, a business case book, and a PKI Interoperability Guide (over 800 pages long).

VI. NEW DRIVERS AND NEW WAYS OF USING PKI

Many of the obstacles faced by traditional PKI can be explained as a misconceived attempt to create a large scale identification regime. It was thought that PKI would support "stranger-to-stranger" e-business. However, new ways of thinking about PKI are based on the context of transactions and the prior relationships that exist between almost all parties doing structured e-business.

The Australian IT Security Forum has observed:

"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 admin and so on. In these cases, users may not know each other personally, but they recognise each other's qualifications. ... Professional qualifications and memberships are more important that personal identity in B2B transactions. Therefore, contemporary PKI almost always involves specific communities of interest. All users have a prior business relationship of some sort." [1]

Other commentators too have recently promoted context-specific digital certificates. For instance, the Chair of the IETF PKIX Working Group recently told the Asia PKI Forum:

"For many big CAs, there is an assumption that a single certificate is all a user should need. This assumes that one identity is sufficient for all applications, which contradicts experience. For personal privacy and security, multiple independent certificates per user are preferable." [3]

Let's look briefly at the evolution of PKI in Australia. This country was an early adopter of PKI. From the mid 1990s there were diverse attempts to use digital certificates in general e-commerce, internet banking, access to telephone accounts, securities stock trading, pension fund online administration, enterprise single sign on, secure e-mail and various B2G schemes. Most of these applications failed, and at the same time, several Certificate Authorities have

gone out of business in Australia. Yet some PKI use cases have survived and are now starting to prosper: tax returns, e-health and customs documentation. These use cases are notable for their "vertical" nature, with well defined contexts and tight controls over participation. Participants tend to have pre-existing relationships, often in the form of government-issued licences or authorisations. In turn this means that risk management and legal liability arrangements are usually in place, which should simplify the implementation of PKI.

Since 2004 we have seen fresh interest in special purpose "vertical" PKI where credentials and prior relationships between parties are more important than the personal identity of individuals. In Australia, there is keen interest in issuing digital "Relationship Certificates" to "Known Customers"; i.e. people who are already well known to the certificate issuer. This new model is the central core of the present reforms to the Commonwealth Gatekeeper PKI Accreditation Scheme [4].

Current real life examples of Relationship Certificate usage from Australia include:

- A large hospital is developing a new "Known Customer" certificate to be issued on smartcards to several thousand staff. The applications include electronic medical notes created by nurses, electronic hospital discharge notes, and employee online services. The hospital administration department will operate a delegated Registration Authority workstation. A Certification Service Provider (CSP) will independently "print" customised certificates and inject them onto smartcards. The same (CSP) will be able to manufacture similar but distinct relationship certificates for other "communities of interest" in the health sector.
- The government is exploring how digital certificates can act as electronic credentials for a number of different types of professionals. A state association for legal professionals is researching how digital "practicing certificates" can be issued to attorneys. The most compelling application for digital signatures in the practice of law is electronic "conveyancing" (real estate property transactions). Electronic conveyancing is forecast to provide direct savings of $70 per transaction for vendors and purchasers, and an overall saving to industry of $33 million p.a. by 2010, assuming 66% of transactions are by then done online[5].
- Most e-health projects anticipate digital certificates. The Australian federal "HealthConnect" project and the New South Wales (provincial) "Health eLink" projects both expect to integrate digital signatures for healthcare providers and, in future, for individual patients too. The Commonwealth is planning a Human Services Smartcard which may have PKI capability, so that it can act as a secure key for accessing sensitive health information.

It is also notable that nearly all of the latest generation national smartcards that have been announced around the world are PKI capable. Many governments - including Austria, Belgium, Estonia, Hong Kong SAR, India, Italy, Kazakhstan and Thailand - plan for increased use of digital certificates to secure their transactions with their citizens, realising like NIST in the USA that PKI offers the only solid solution to website fraud and phishing. [2]

V. PKI IN PLAIN LANGUAGE

One of the top four findings of the OASIS PKI Surveys in 2003 was that PKI advocates have focused too much on the technology and not enough on the benefits [6]. Most PKI vendors publish detailed technological white papers and FAQs. Many offer exhaustive technical training courses on cryptography and PKI. This fascination with technology is probably unique to our industry. Yet it is possible to explain the benefits of PKI in plain language. We can tell a layperson everything they need to know, in just a few paragraphs, as follows:

A smartcard plus special application software combine to produce digital signature codes for electronic

transactions. Unlike any other electronic signature method, digital signature codes are unique to the owner and also to each transaction. Digital signatures operate as if a personalised electronic stamping machine was inside each smartcard, creating a specific 'mark' on each message or file created by the card holder. Digital signatures remain valid indefinitely; that is, at anytime in future, the 'mark' can be easily verified to prove its origins.

Digital certificates are electronic notices that bind individuals to smartcards and thence to transactions signed using their smartcards. A digital certificate can identify the card holder and can also hold any other information about the holder that the issuer is qualified to declare. If the issuer is authoritative over information such as professional credentials, then that information can be sealed within its digital certificates and thus bound to each card holder.

To process digitally signed transactions, the receiver's software requires a copy of the sender's certificate, plus a special "master code" - known as a root certificate - which is used to mathematically validate all certificates in a given PKI scheme. Different master codes define different PKI schemes, be they sector-specific, national or general purpose such as SSL website authentication. Application software can ship with all necessary master codes, or can have them installed later.

Digital certificates can be electronically revoked at any time. Revocation may be requested by the holder in the event that they lose their smartcard. Alternatively, revocation of a professional's certificate may follow automatically from their membership lapsing or their qualifications being cancelled.

VI.PKI AND COMBATING WEB FRAUD

One of the most dangerous vectors for web fraud today - including phishing and counterfeit ghost sites - is the "Man In The Middle" attack (MITM). A non-technical explanation of MITM and an analysis of the abilities of various security technologies to deal with it are provided in [7].

Under Homeland Security Presidential Directive HSPD-12, the US Government is about to roll out some 10 million smartcards for identifying federal employees and contractors. New federal information processing standard FIPS-201 (available at www.nist.gov.au) mandates sophisticated PKI functions in these smartcards for the purpose of remote authentication. PKI smartcards (or alternatively USB keys) have been described by the head of cryptography at the US National Institute for Standards and Technology as the "only practical solution today" for MITM [2].

Thus PKI is emerging literally as the key to safe access to online services.

VII. A CLEARER ROLE FOR REGULATORS

As discussed, PKI commentators are increasingly expressing the view that public key technology is better suited to application-specific electronic credentials than to general purpose identification. An implication of this viewpoint is that e-business users can have different identities in different transaction contexts. What should the response of regulators be to these developments? Australia looks like being one of the first jurisdictions to take the next logical step.

The outcomes of the recent Gatekeeper Review include a recommendation that for certain types of transactions, digital certificate holders could be registered on the basis of a demonstrated relationship with the certificate issuer instead of traditional in-person identity checking. The word for this type of certificate subject is "Known Customer" in relation to the issuer [4]. A major strategic implication of the Known Customer model for PKI regulators is regulators now have less to say about how business partners should know one another [8]. Under Known Customer certificate issuance, regulators would allow parties to establish trust in one another's identities according to their own business rules, in a manner that is fit for the intended purpose of the certificates [9].

For example, if a qualified medical doctor carries an authorisation or a licence to practice issued by an authoritative health care body, then a Known Customer digital certificate can be issued to that doctor without additional in-person identity checks. It is of course necessary to take steps to prevent Known Customer certificates from falling into the wrong hands, but these steps do not have to involve new identity checks.

Most PKI accreditation and licensing programs have prescribed personal identification benchmarks comparable to traditional passports. But it is not a necessary role of regulators to prescribe identity benchmarks for all types of online transactions. Instead, identity standards should be business decisions made by the transaction scheme operator using risk management principles. In vertical transaction schemes like trade documentation and e-health, the operator has to make all sorts of technical risk management decisions, including the design of software user interfaces and application access controls. The user registration procedure should be treated as just another one of these types of risk management decision. Then it is possible for the PKI regulator to step away from mandating identification benchmarks.

The fundamental value of PKI accreditation is to convey a quality endorsement of some kind, and to facilitate interoperability between e-business parties and applications. PKI regulators do not need to specify identity vetting rules in vertical PKI schemes. Instead they can publish identity vetting guidelines, in order to improve interoperability via transparency and high operational standards.

Note that for national identity PKIs naturally the regulator will find it important to set identity checking benchmarks comparable to passports, to ensure uniformity. The "Relationship Certificate" principle simply says that for certain types of vertical PKI schemes (also known as "closed" or "open but bounded" PKIs) the regulator should leave all risk management decisions to the business operators.

VIII. CONCLUSIONS

There are a number of steps that governments, regulators and PKI service providers can now take to promote better application of digital certificates, and to improve the way that PKI is regulated. In conclusion, the author recommends that the following steps be given consideration by those concerned with PKI governance.

- Continue with PKI reforms, such as the Australian Gatekeeper reforms, in order to facilitate new and improved digital certificate applications; in particular, mechanisms should be examined for managing Known Customer issuance and Relationship Certificates, for the benefits of major cost reduction in user registration and more streamlined distribution of certificates.
- Relationship Certificates can be manufactured automatically on a wholesale basis by Certificate Service Providers (CSPs) on order from trusted organisations' RAs. CSPs providing Relationship Certificates can be divorced from all identification risks and application risks, thus minimising their costs [10]. This leads to a simpler business model, faster start-up of new PKI enabled applications, and a clearer basis for accreditation of CSP operations.
- Cross border PKI recognition could be facilitated via Mutual Recognition Arrangements already in place across Asia for technology evaluation. The Asia Pacific Laboratory Accreditation (APLAC) supervises a range of interoperable evaluation programs under the international Requirements for the Competence of Calibration and Testing Laboratories ISO 17025. These could be extended to PKI so that Relationship Certificates manufactured by any approved CSP in Asia could be replied upon in any APLAC jurisdiction, within an established and transparent liability framework.

REFERENCES

[1]. Position Statement on PKI of the Australian

Security Industry 2003; http://www.aitsf.aeema.asn.au/ArticleDocuments/175/pki.pdf.

[2]. Electronic Authentication in the U.S. Federal Government Bill Burr, Manager Security Technology, National Institute of Standards and technology, Asia PKI Forum, Tokyo, February 2005 http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf.

[3]. Global PKI: Status, Trends and the Future Dr. Stephen Kent, co-chair IETF PKIX Working Group, Taipei International PKI Conference, September 2005.

[4]. Draft Gatekeeper Public Key Infrastructure Framework http://www.agimo.gov.au/__data/assets/pdf_file/46135/Gatekeeper_PKI_Framework.pdf.

[5]. Land Exchange (LX) Case Study, Government of Victoria, July 2004, http://www.egov.vic.gov.au/pdfs/Land%20Exchange-shh-30April-v1.0-CIO.pdf.

[6]. Analysis of August 2003 Follow-up Survey on Obstacles to PKI Deployment and Usage OASIS PKI Technical Committee, October 2003; www.oasis-open.org/committees/pki/pkiobstaclesaugust2003surveyreport.pdf.

[7]. A unified solution to identity theft, Stephen Wilson, Lockstep Consulting, http://www.lockstep.com.au/library/identity_authentication/towards_a_uniform_solution.

[8]. Relationship Certificates for Known Customers - a New PKI Paradigm Stephen Wilson, Asia PKI Forum 5th International Symposium, Beijing, 5 November 2005; available at http://www.lockstep.com.au/library/conference_presentations.

[9]. Relationship Certificates: a modified form of identity certificate for conveying credentials Stephen Wilson, August 2005, Lockstep Consulting White Paper http://www.lockstep.com.au/library/pki/relationship_certificates

[10]. The Security Printer model for CA Operations, Stephen Wilson, August 2005, Lockstep Consulting White Paper www.lockstep.com.au/library/pki/the_security_printer_model_fo.

1. Note in particular that password based Internet banking still features "non-repudiation": it is very difficult to falsely deny making an Internet banking transaction. Therefore we see that "non-repudiation" is not a unique feature of PKI.

BIOGRAPHY

Stephen Wilson *is a leading independent authority on PKI, identity management and information security. He is a long time member of the APEC eSecurity Task Group, and a member of the Board of Directors of the Australian IT Security Forum. Currently he is a member of the OASIS PKI Technical Committee and is the elected liaison representative of OASIS to the Asia PKI Forum. He was an original member of the National Electronic Authentication Council (NEAC), an invited member of the Australian Federal Privacy Commissioner's PKI Reference Group, and Chair of the Certification Forum of Australasia from 1998 to 2001.*

In January 2004, Stephen founded Lockstep Consulting Pty Ltd. He provides independent advice and analysis on PKI and smartcards to clients all around Asia.