Lockstep Consulting Pty Ltd
11 Minnesota Ave
Five Dock (Sydney) NSW 2046
Australia

Asia PKI Forum Members Meeting Tokyo Feb 2005
Trip Report for OASIS PKI TC

Stephen Wilson
Director, Lockstep Consulting
OASIS Liaison to Asia PKI Forum
May 2005

Executive summary

The 4th quarterly Steering Committee and Working Group meeting for FY2004 of the Asia PKI Forum was held in Tokyo over February 21-23. The Asia PKI Forum public conference followed on February 24. Stephen Wilson represented the OASIS PKI Technical Committee at these meetings, and made two presentations on behalf of OASIS (PowerPoints attached)

This was the first time OASIS had participated in the APKIF; I was warmly welcomed all round. The APKIF is actively expanding its catchment area and seeking to increase its influence (details below); therefore there is high interest in the experiences of the OASIS PKI TC in general and our future survey plans in particular. Tangible commitment at their end to the relationship is demonstrated by the appointment already of two liaison representatives.

Highlights

Here is a personal reflection on the highlights of the meetings and conference.

— The search for killer applications continues to preoccupy PKI efforts worldwide. The importance of case studies, practical guidance, cost minimisation, and genuine value propositions was just as notable in the APKIF as it is in OASIS.

— Yet interest in PKI is increasing strongly; most people I spoke to in essence recognise the ‘trough of disillusionment’ of the past few years and agree that PKI is now resurgent.

— The APKIF is actively expanding its catchment area, and similar fora seem to be proliferating again, across Asia as well as Latin America, after the lull of recent years. Mexico, Vietnam and Malaysia were all mentioned as being well advanced in establishing national PKI fora. APKIF is also targeting India.

— The strongest areas for immediate collaboration between APKIF and OASIS appear to be in the areas of resources (sharing case studies and business cases) and ongoing surveys. These activities fall under the APKIF's Business Application Working Group and International Cooperation Working Group.

— The nominated liaison representatives from APKIF to the OASIS PKI TC were announced as Dr Wen-Cheng Wang from Chinese Taipei and Mr Kiyoshi Watanabe form Japan.

— APKIF's strategic plans also include the establishment of a Consulting Services team comprising nominated experts from member fora. A directory of experts across the region is being compiled (as well as a directory of PKI vendors). The team is envisaged to be available for awareness programs, training and specialist consulting.

— No clear consensus has yet to emerge across Asia on PKI regulations and governance. Most Asian economies have either *prescriptive* PKI legislation (where digital certificates from accredited CAs are mandated for e-commerce; e.g. Malaysia, India) or two tier legislation (where digital signatures are not mandated but do confer certain legal advantages; e.g. Singapore, Hong Kong China, Chinese Taipei, Korea, Thailand). Important cross-border interoperability programs are underway in the area of trade documentation (the Pan Asia Alliance, a closed mutual recognition arrangement) and in general e-commerce in the 10 ASEAN member states (under the open harmonisation project of eASEAN).

— While a relatively high degree of government involvement is expected across Asia (as indicated by the prevalence of prescriptive and two tier legislation), the precise role of government has yet to emerge. In Singapore for example, where PKI applications are generally thriving, there is only one government licensed CA. Most commercial CAs forego licensing to keep costs down, relying on contracts rather than legislation to manage their risks.

— Smartcards – often with public key capability – are penetrating rapidly across Asia. In Chinese Taipei, most adults have at least two different smartcards in their wallets (one for health insurance, and one or more for banking). An optional personal digital certificate smartcard from government has been obtained by nearly a million citizens.

— The full potential of PK-capable (or EMV type) smartcards to act as containers for one or more digital certificates seems to have not yet sunk in, in spite of the popularity of smartcards in general. The Asia Pacific Smartcard Association does not yet have a vision for how PKI relates to its activities or its members' interests. There may be an opportunity here for collaboration in developing and articulating new types of PKI applications on smartcards.

— The cable TV industry PKI (of "OpenCable") was discussed in the context of embedded PKI. I have not had any exposure to OpenCable until now; it strikes me as one of the biggest PKIs anywhere worldwide, with millions of certificates embedded in set-top boxes, and manufacturers having their own CA functions. OpenCable may be worthy of further examination by OASIS PKI TC, as a case study, and/or area for collaboration

Background and Explanatory Notes

Newcomers to Asian geopolitics must take note of some special nomenclature. The APEC (Asia Pacific Economic Cooperation) forum has adopted certain naming conventions that reflect the history and cultural sensitivities of the region. Many other organisations have adopted the APEC terms.

Firstly, it is common not to refer to "countries" but rather to "economies". And certain Western names are deprecated, and replaced as follows:

— Taiwan is referred to as *Chinese Taipei*
— Hong Kong is referred to as *Hong Kong China*
— Macau is referred to as *Macau China*
— South Korea is referred to simply as *Korea*.

In APEC it is considered undiplomatic to not use the italicised terms above. It seems best to use the same conventions in dealing with the Asia PKI Forum.

Asia PKI Forum Structure and Activities

All members of the APKIF are national PKI fora. Current members come from China, Hong Kong China, Japan, Korea, Macau China, Singapore, and Chinese Taipei. Thailand too was active at the February meetings.

The APKIF carries out most of its work in four Working Groups:

1. ***Business Case & Applications*** (BAWG) chaired by Chinese Taipei,
2. ***Interoperability*** (IOWG) chaired by Japan,
3. ***Legal Infrastructure*** (LIWG) chaired by Japan and a new co-chair from Chinese Taipei, and
4. ***Worldwide Collaboration*** (WWCWG) chaired by Chinese Taipei.

The schedule of meetings for the next 12 months is:

— ***Singapore*** July 5-6
(see http://asia-pkiforum.org/NEW/03_event/july_singapore.php)
— ***Chinese Taipei*** September
— ***China*** November
— ***Korea*** March 2006

There have been three major deliverables from the APKIF to date: a detailed set of technical Interoperability Guidelines, a detailed analysis of legal issues in member economies, and a study of CA liabilities in cross-border e-commerce (see *Attachments* at the end of this paper).

The APKIF homepage is at http://www.asia-pkiforum.org.

Specific potential collaborations

In summary, the following are the most likely areas for immediate and mutually beneficial collaboration between the APKIF and OASIS:

1. International PKI surveys (some budget has been allocated by APKIF)
2. White papers and publications (for the APKIF Business Case Book)
3. The new OASIS PKI resources web pages

APKI Conference Summary

Most presentations from the conference are available at http://asia-pkiforum.org/feb_tokyo/index.htm.

The conference was well attended, with roughly 100 delegates. It was a free event, held at a Tokyo university; while many delegates were students, clearly many were business people too.

A panel discussion on PKI around the region was my main involvement in the conference proper (as distinct from the Working Group sessions). On the panel I was joined by representatives from China, Korea, Singapore and Chinese Taipei. The overall tone of the panel was cautious optimism. The search for killer apps continues. For instance, even with over 8,000,000 certificates (mostly soft keys) issued by Korean banks, the Korean delegate expressed reservations about the "success" of PKI so far.

Smartcard adoption is seemingly highest in Chinese Taipei. All banks there were required by the regulator last year to switch from magnetic stripe to chip to combat skimming (though only a minority of the bank cards are EMV compliant, due to cost concerns). Also, every Chinese Taipei adult has a national health insurance smartcard, and nearly a million have elected to have a general purpose PKI card as well. Smartcard readers are not yet widespread in standard PCs and laptops, but USB readers are readily available, from outlets including Seven-Eleven stores!

Bill Burr from NIST delivered one of the key notes. In the context of the US Federal id standard FIPS 201, he advocated smartcards for remote authentication, as the "only practical solution" today for combating Man In The Middle attack and account hijacking. Bill also commented that biometrics remain difficult to implement for remote authentication, as well as in unsupervised modes.

The Asia Pacific Smartcard Association presented a raft of detail on cards and related fraud across the region. His presentation is available at the conference website; my summary is immediately below.

Notes on ATM card fraud

Card fraud by skimming and cloning is increasing across the region. Organised crime gangs have set up sophisticated "carding" operations, where large numbers of counterfeit cards are produced replicating stolen customer information. In a famous case in Malaysia, it was found that criminals had tapped the telephone trunk lines leading out of a major shopping mall, enabling them to eavesdrop on credit card authorisations and thus quickly capture the magnetic stripe data for many thousands of customers.

The response by regulators in certain jurisdictions has been to set relatively aggressive migration targets for chip cards, which are essentially immune from counterfeiting. Most notably, Malaysia, Chinese Taipei and Korea have already imposed deadlines in or before 2005. In Chinese Taipei, the regulator initially sought a six month transition period from magnetic stripe to chip, although the banks managed to negotiate an extension to 12 months.

EMV migration across Asia

In Asia, EMV and national payments organisations recognise two tiers in the regional market. Japan, Korea, Malaysia and Chinese Taipei are the upper tier; Thailand, Singapore, Hong Kong China and Australia are the lower tier. With smartcard ticketing and advanced telephone services being further advanced in Asia than in other parts of the world, there is strong interest in bank-issued cards being multi-application.

Combating card fraud tends to make the business case for EMV migration in Japan and Chinese Taipei. On the other hand, in Korea card fraud is relatively low, and the banks' interest in smartcards is driven by competitive product differentiation, where loyalty, calling card and/or ticketing options are available on multi-application chip platforms. In Malaysia, card fraud remains manageable for domestic bank customers but for foreign issued credit cards, fraud is rampant. Therefore it is expected that Malaysia will ironically be the first Asian country to complete EMV migration.

The table below summarises EMV progress in most of the tier one markets.

Market	**EMV cards**	**EMV terminals**
Japan	20 million	39,000
Chinese Taipei	2 million	80,000
Korea	2 million	No data presented

APKIF Working Group Summaries

Business Case & Applications

The BAWG's major ongoing activity is the production of a Business Case Book, the next iteration of which is likely to include a new survey on cross border PKI. The Working Group is canvassing members (and OASIS) for contributions. Other plans and work items include a forthcoming newsletter, and a PKI merchant directory.

Interoperability

This was the best attended Working Group, possibly reflecting the depth and quality of the work done to date on the Interoperability Guidelines.

The IOWG invited OASIS to make a presentation on interoperability at the next meeting.

For three years, the IOWG has been carrying on an interoperability experiment, with the effort largely underwritten by the Japan PKI Forum. Progress has been fitful, due to the absence of any full time staff dedicated to the project.

I presented an overview of the OASIS PKI Action Plan, which was well received. I suggested that the focus of interoperability work in future should probably be on certificate management protocols and on private key media interface issues, especially in respect of smartcards. The IOWG Chair agreed, citing the increasing importance of smartcards in Japan and across Asia.

Legal Infrastructure

The LIWG was a short meeting, concerned mainly with putting the finishing touches on its major recent deliverable, the report "CA Responsibilities and Liability for Cross-Border E-Commerce" (see draft attached).

Next LIWG projects are proposed to include an examination of how CAs can manage the risk of new and disruptive technologies, specifically RFID and biometrics. They may also look at new chip enabled passports.

Worldwide Collaboration

One of this WG's major efforts was the APKIF booth at the 2005 RSA Conference, which was thought to be a great success.

- They formally recorded over 300 visitors at the booth.
- They have compiled a list of frequently asked questions (including "Is the Asia PKI Forum a bridge CA for Asia?", "Does the APKIF accredit Cas?" and "How do I search for vendors in Asia?").
- The APKIF's legal infrastructure report was well received, indicating strong demand for this type of resource worldwide.

The WWCWG's plan for the rest of the year includes:

- Setting up a Consulting Services team
- Promoting APKIF events
- Pursuing collaborations with OASIS, the APEC eSecurity Task Group, the European Electronic Messaging Association (EEMA), the Pan Asia Alliance (PAA) and the European Electronic Signature Standardisation Initiative (EESSI)
- Expansion in general, targeting firstly Vietnam and Malaysia.

Miscellaneous regional highlights

Japan

There is an ambitious program by local government prefectures across Japan to issue PKI based residential cards to essentially every adult. Estimates of the volume to date vary between 300,000 to nearly a million cards. There is some official disappointment at the take up, though there is still no killer app to make the cards compelling.

A smartcard for healthcare professionals is rolling out, with 70,000 issued so far.

Korea

Internet banking in Korea (unlike the rest of the world) is the killer app for PKI. To date, the six largest banks have issued 10 million certs (out of a total population of 45M).

Singapore

The government agency iDA, responsible for the Controller of CAs, is said to be cutting its budget, in the wake of lower than expected demand for licensed CAs (only one licence has been issued).

Chinese Taipei

22 million PK-capable health insurance smartcards;
700,000+ govt issued general purpose PKI smartcards

Some useful links

APKIF homepage	http://www.asia-pkiforum.org
Asia PKI Forum conference	http://asia-pkiforum.org/feb_tokyo/Forum.htm
Open Cable PKI	www.opencable.com (and search for "PKI")
Pan Asia Alliance (PAA)	www.paa.net

Attachments

The Oasis PKI Action Plan (Stephen Wilson PowerPoint presentation)
PKI lessons from Australia (Stephen Wilson PowerPoint presentation)
Asia PKI Interoperability Guideline (V 2.0, Draft) Books 1 & 2 (by APKIF IOWG)
CA Responsibilities and Liability for Cross-Border E-Commerce (by APKIF LIWG)