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

Asia PKI Forum Members Quarterly Meetings Singapore July 2005 Trip Report for OASIS PKI TC

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

August 2005

Executive summary

The first quarterly Steering Committee and Working Group meetings for FY2005 of the Asia PKI Forum were held in Singapore over July 5-7. This was another exciting and well attended gathering. The APKIF membership continues to grow strongly. Vietnam has recently been admitted (as an affiliate) and sent three delegates to Singapore; Thailand sent five representatives; newcomer Kazakhstan attended with one observer.

Major deliverables continue to emerge from APKIF. They had just published Book Three of the Interoperability Guide which now totals 834 pages! The latest installment addresses CA security benchmarks, licensing and compliance frameworks in detail, across seven Asian jurisdictions. A business case study book is also at an advanced draft stage.

With legal infrastructure and low level interoperability issues now well covered, the emphasis in APKIF seems to be shifting (sensibly) to implementation strategies. There are opportunities here for OASIS and APKIF to collaborate. Smartcards were again a hot topic, with much discussion of their use not only for national ID and payments but also for generalised entitlements and membership control; for example, in Taiwan up to five million high grade smartcards (FIPS 140-2) will be issued to online gamers for authentication

I delivered a verbal report in Singapore on the OASIS PKI action plan, the ROI White paper and the new website, which was especially well received. We can expect requests to add new links from APKIF and other external groups.

Update on APKIF Membership and Activities

General business

The position of Chair of Asia PKI Forum passed to China at this meeting.

Vietnam has been confirmed as an Affiliate Member of APKIF.

Business Case & Applications Working Group

The Business Case Book in its current draft has reached about 50 pages. The BAWG is very keen to share case study materials with OASIS.

Another BAWG activity is the planned regional capability directory.

A very good presentation of various projects in Singapore by Crimson Logic (including the very interesting and significant Electronic Certificate of Origin project) included their observation that XMLsignatures does not support multiple signatures very well, whereas XPath does.

Interoperability Working Group

Book Three of the Interoperability Guide details CA licensing across seven Asian jurisdictions: China, Honk Kong China, Japan, Korea, Singapore, Chinese Taipei and Thailand. The book digs all the way into respective competent authorities, liability arrangements, audit requirements, CA key generation specs, user key management, and subscriber "safety" provisions.

My impression is that the Guide Book's 'frame of reference' has to do with cross-certification and that the whole exercise therefore is one of Certificate Policy mapping. In my view, this is not necessarily the most effective road to interoperability but nevertheless this work is a superb resource for anyone interested in how PKI is regulated in many especially important places such as Japan and China.

The IOWG plans to now work towards pilot projects, and to examine how new applied technologies like e-passports can make better use of interoperable PKI.

The Chinese Taipei PKI Forum reported to IOWG the formation of a new government funded PKI test-bed, which may be opened up to other Asia PKI Forum members.

Legal Infrastructure Working Group

The LIWG's latest research questionnaire concerns new technologies – including biometrics – and their potential to disrupt PKI.

Worldwide Collaboration Working Group

The WWCWG is generally responsible for APKIF's survey activities. These have not progressed since the February meetings, but it is hoped that with the acceleration of the OASIS Lower Costs SC work, that collaborative international surveys will emerge soon.

General notes

There were some 30 to 35 representatives at the Working Group meetings, plus at least 10 guests 'in the galleries' at most sessions.

An indicative contemporary use of PKI smartcards for entitlement management is Chinese Taipei's "Play Safe" card for online gaming. The smartcard is a FIPS 140-2 rated device, costing some US$12 each. Readers are an extra US$6 a piece. Players are charged $1.50 per month for the card and reader. Up to 10,000 cards have been deployed so far, with numbers expected to grow to 5,000,000.

Macau China has its new electronic signature legislation drafted and undergoing government approval. Their CA is technically operational, with legal and administrative particulars still under development.

Thailand has launched its e-Passport. A separate project is their national ID smartcard, for which the first 8 million smartcards have been ordered, with many more to come in later stages.

Kazakhstan's observer was primarily interested in strategic questions about the value proposition for including PKI capability in their planned national ID smartcard. Specifying a crypto card has obvious cost implications; they are exploring whether the capability to deliver PKI-enabled applications using the smartcard can make the cost worthwhile.

Vietnam envisages a national PKI system, sponsored by the government, and is in the process of scoping such a capability and better understanding the requirements.

Annex: Background to the Asia PKI Forum

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. The Asia PKI Forum generally uses the APEC jargon. Generally, it is common not to refer to "countries" but rather to "economies". And certain Western names for Asian countries 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*.

All members of the APKIF are national PKI fora. Current members come from China, Hong Kong China, Japan, Korea, Macau China, Singapore, Chinese Taipei, and Vietnam.

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

1. ***Business Case & Applications*** (BAWG)
2. ***Interoperability*** (IOWG)
3. ***Legal Infrastructure*** (LIWG, and
4. ***Worldwide Collaboration*** (WWCWG).

The next few meetings are scheduled as follows:

— ***Chinese Taipei*** September 13-15;
see http://asia-pkiforum.org/NEW/03_event/sept_taipei2005.php.

— ***China*** November

— ***Korea*** March 2006

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