Trip Report
Asia PKI Forum 1st FY06 Working Group Meetings
and the Asia PKI Forum 6th International Symposium
Chengdu, China, July 2006

Stephen Wilson (swilson@lockstep.com.au)
OASIS PKI Technical Committee Liaison representative to APKIF

The first quarterly Steering Committee and Working Group meetings for FY2006[1] of the Asia PKI Forum were held over July 25-26 in Chengdu in the Sichuan province of China. The Forum's 6th International PKI Symposium followed on July 27.

The Asia PKI Forum is on the verge of significant change. The Forum, after an internal strategic review, has decided to broaden its focus to e-commerce security more generally, and will likely change its name and charter in the next six months. In an unrelated development, the Japan PKI Forum has announced it will withdraw from APKIF by June 2007.

I provided the final version of the Third OASIS PKI survey to the World Wide Collaboration Working Group (WWCWG), and the Memorandum of Understanding for OASIS-APKIF collaboration on the survey. The WWCWG undertook to review and sign-off the MOU in the next few weeks, and have agreed to promulgate the questionnaire amongst APKIF members.

Most progress in the past six months has been made by the Legal Infrastructure Working Group (LIWG) which handed down a near final draft of its wide ranging survey of security regulations and new technologies, and by the Interoperability Working Group (IOWG). The IOWG presented a proposal to develop a new Framework for Interoperability Evaluation Criteria, and an associated Certification and Accreditation laboratory. They have based their interoperability measurement objectives on some very sophisticated concepts of what types of information are needed for different purposes or "consumers" of certificates, and WWCWG members broadly supported this aspect of the work. However, the proposal to invest in a new lab was controversial, because it seems to cut across existing legislated as well as private sector accreditation regimes.

The PKI symposium featured a rich set of international presentations, including Cisco, Fujitsu Research, Intel, iTrusChina (Verisign's Chinese affiliate), KPMG, Sterling Commerce, and myself. Perhaps the most interesting papers were by Microsoft (showing how PKI is realised in the new Identity Meta-system) and by Korean systems integrator Softforum (looking at television-mediated transactions, or "t-commerce", where certificates are used from set top boxes).

Update on APKIF Membership and Activities

Legal Infrastructure Working Group (LIWG)

The LIWG's most recent major deliverable was tabled: *Legal Issues on New Security Technologies and*

---

[1] Please note the APKIF fiscal year convention, where FY"200X" runs from July 200X to June of the following year. This is different from the typical western fiscal year naming convention.

CA's Risk Management. Input was provided from China, Japan, Korea, Singapore, Chinese Taipei, Hong Kong, Macao, Thailand and Australia. This work surveyed a wide range of security issues, including plastic card fraud, biometrics, spyware and so on (according to a questionnaire circulated previously to the OASIS PKI TC).

Business Case & Applications Working Group (BAWG)

The BAWG has found it difficult to gather sufficient case studies to make its *Business Case Book* worth pursuing, and so has decided to terminate this activity. It has however continued to compile a regional experts list from Asia PKI Forum members. An international training course was held in Taipei, and there are plans to repeat the course in association with the next APKIF working group meetings in November.

Interoperability Working Group (IOWG)

There were no technical presentations at the Chengdu IOWG session, unlike previous meetings. The main agenda item this time was a proposal originating from China to develop a new set of Interoperability Evaluation Criteria, and a framework and laboratory for formally measuring CAs against the criteria.   The presentation in my view included a very sophisticated account of the different types of information that need to be disclosed through certificates (and other channels) to "consumers" of certificates (what is traditionally call the Relying Parties). They distinguish three aspects of the information conveyed via certificates: it must be (1) understandable, (2) adequate and (3) trusted.

However, more controversial is the IOWG's belief that a useful *Interoperability Capability* can be measured quantitatively[1] and moreover that it would be useful to build a Certification & Accreditation Laboratory. Because it is not clear yet how such a new lab would relate to existing legislated licensing schemes (such as those in India and Singapore) and private sector schemes (like WebTrust), IOWG members did not support this aspect of the proposal so strongly.

Worldwide Collaboration Working Group (WWCWG)

I tabled the Memorandum of Understanding from OASIS, for review and approval by the WWCWG as a prelude to us working together on the 3rd International PKI Survey. Interest in this exercise remains strong in the Asia PKI Forum. A practical problem in our collaboration has surfaced however: the next APKIF Working Group meetings and conference will not be until November, which is rather later than we had hoped, relative to the planned duration of the survey.

---

[1] In my personal opinion, this approach is fraught, because in most vertical PKIs today, the Relying Party question is simply whether to accept or not (that is, it is binary, not numerical) and moreover is enacted by machines in real time, not by humans referring to test results for new CAs.

General Meeting of the APKIF

There were two pieces of unexpected news at the General Meeting. Firstly, the APKIF has in the past few months undertaken an internal strategic review, under the auspices of a specially convened "transformation" working group. The result is that the Forum is to broaden its focus to encompass all of e-commerce security, not just PKI. A name change and revised charter are expected shortly. The transformation was also reported to be aimed at facilitating contributions from a wider set of affiliates.

Secondly, the Japan PKI Forum announced that it was going to withdraw from APKIF at the end of the current financial year. They reported that their members felt the APKIF had achieved their major deliverables, and that members' resources could be better deployed now in other ways.

The APKIF 6th International Symposium

This event was held after the Working Group and Steering Committee meetings, and was attended by over 200 delegates. Conference highlights for me included:

- A case study from Korea on "t-commerce" (that is, television commerce) involving digital certificates loaded into set-top boxes; the private keys are transferable to and from other devices such as smartcards, PDAs, cell phones and so on.
- KPMG Hong Kong described the increasing importance of CA audit in the region.
- Microsoft China presented InfoCard and the Identity Meta-system, emphasizing the emerging acceptance of there being multiple identifiers, and the good fit with new PKI models.

My presentation concerned embedded PKI, and canvassed recent examples such as Skype and medical professional smartcards. It draws a comparison between PKI embedded in smartcards and comparably complex ferromagnetic technologies intrinsic to familiar plastic cards, making use of the OASIS digital certificate supply chain model. The slides will be posted to the PKI TC members pages.

OASIS PKI

Annex: Background to the Asia PKI Forum

Terminology

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*.

Constituents

All members of the APKIF are national PKI fora. Foundation Members are China, Japan, Korea, Singapore and Chinese Taipei. Other members are Hong Kong China, India, Macau China and Vietnam.

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

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).

Upcoming meetings

The remaining FY06 meetings are as follows:

Chinese Taipei	Nov 9-10
India	March 2007 (To Be Confirmed)