Trip Report
Asia PKI Forum 3rd FY05 Working Group Meetings and the Asia PKI Forum 5th International Symposium
Beijing, November 2005

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

The third quarterly Steering Committee and Working Group meetings for FY2005 of the Asia PKI Forum were held in Beijing over November 3-4. The Forum's 5th International Symposium followed on November 5. There were also visits organized to two major Chinese PKI companies.

I presented the near final beta version of the Third OASIS PKI survey to the World Wide Collaboration WG, and it was well received. The survey has subsequently been distributed to all WWCWG members, with a request for feedback and for target respondents to be nominated. Additionally, Dr Riccardo Genghini, chair of the European Electronic Signatures & Infrastructures Technical Committee, plans to table the OASIS survey with his committee later this month and will ask for their support.

The WWCWG and the Legal Infrastructure Working Group both asked for contributions from OASIS for their respective projects, the PKI Business Case Book and Legal Issues in New Security Technologies. Supporting documents are attached to this report.

The Interoperability Working Group (IOWG) had separate presentations from Korea and Japan which argued respectively for X.509 certificates to convey long term attributes, and for the registration function for certain types of certificates to move from generic certificate service providers to "trusted organisations". These proposals resonate with experience in Australia with "Relationship Certificates". My invited presentation to the Symposium was also on Relationship Certificates, and it was very well received.

Update on APKIF Membership and Activities

Legal Infrastructure Working Group (LIWG)

The LIWG's sole effort at present is research into "Legal Issues on New Security Technologies and CA's Risk Management". A questionnaire circulated in September at the Taipei meeting is slowly attracting responses. The first draft report was tabled in Beijing, incorporating responses from just Japan and Korea so far. At the meeting I submitted an informal response concerning Australia.

LIWG Chair Mr Hiro Rokugawa is keen for the request form to be answered for as many jurisdictions as possible, including the US. **The PKI TC should therefore consider compiling a response for the US at least. I propose we discuss on our next conference call.** The response form is attached.

Business Case & Applications Working Group (BC/APWG)

One of two main activities of the BC/APWG's is the ongoing compilation of its *Business Case Book*. At the Beijing meeting, the WG Acting Chair was very keen for cases to be submitted from around the world, outside Asia. **Individual OASIS PKI TC members are therefore invited to compose brief accounts of PKI applications (around two to four pages long) and to submit them to me on behalf of the BC/APWG.** The latest draft of the Case Book is attached; submissions should be structured as follows:

1. Business background
2. Structure of the case
3. System configuration
4. Effects
5. Further developments
6. Other issues

The WG's other main activity is the development of a significant PKI Training Program (driven by the BC/APWG's thesis, shared of course by the PKI TC, that poor understanding of PKI is a major obstacle to its take-up). A five day course is tentatively scheduled for February 20-24. Topics are to include technology, applications, international trends, policy and law, accreditation and operational issues.

Interoperability Working Group (IOWG)

As foreshadowed at the Taipei meeting, the latest IOWG meeting consisted mainly of technical presentations from members. The main topics included:

- A scheme for safeguarding national identity numbers by combining them with random data and sealing them into digital certificates in the SUBJECT ALTERNATE NAME field (Koreas). Dr Genghini remarked that a similar method is used in the Austrian national smartcard.
- A proposal for "Next Generation E-Authentication" which is "characterized by making 'trusted organization' perform the user registration procedure and authentication instead of a service provider in order to protect a user's personal information" (Japan). That is, instead of registering all PKI users via third party general identity services or traditional CAs, in some cases it may be better to have trusted authoritative bodies do the job. This proposal resonates strongly with the "Relationship Certificates" model advanced by the current Gatekeeper reforms in Australia; see www.agimo.gov.au/__data/assets/pdf_file/46135/Gatekeeper_PKI_Framework.pdf and www.lockstep.com.au/library/pki/relationship_certificates.
- Investigations into cross recognition by iTRUS are proceeding along two directions: Validation Authorities and Trust Lists as defined by the APEC eSecurity Task Group (China).
- Conveying long term attributes through conventional X.509 certificates rather than Attribute Certificates, the latter being more complex and in need of additional infrastructure (Korea). Like the Japanese proposal above, this concept too aligns with the Australian Relationship Certificate model.

Worldwide Collaboration Working Group (WWCWG)

A major part of the WWCWG agenda was my presentation on the OASIS Lower Costs SC Survey (PowerPoints attached). One delegate said he thought the survey was 'the best he had ever seen'. There was strong overall support for the WWCWG to be involved. In depth discussion followed, with much valuable feedback, including:

- To support collaboration on the survey in Asia, it will be useful to have a statement that clearly sets out the actions expected from OASIS and APKIF.
- It might be worth considering offering honoraria or tickets in a prize draw in consideration of those people who volunteer to be interviewed.
- We need to make sure there are no IP complications in the event that the APKIF would seek to modify the questionnaire for local use.
- We should promote the survey into the new Africa PKI Forum, and any comparable Latin American organisations.
- Riccardo Genghini plans to table the questionnaire at his ETSI Electronic Signatures Committee meeting at the end of November. He is a strong supporter.

The APKIF 5th International Symposium

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

- The Italian Registry of Companies is now wholly digital. The only way for companies in Italy to update their records, or for the public to view current public records, is to go online. Some 2.5 million hard certificates (issued to tokens that comply with Europe's tough *qualified electronic signature* requirements) are used regularly by companies to lodge official statements and reports.
- Riccardo Genghini strongly supports the Austrian national smartcard for its special ability to de-identify holders for many transactions. The holder's name is not featured on the card, but instead may be linked at the back end when required for a given transaction. He regards it as a crucial but still rare move by government away from identity PKI towards what in Australia is called "Relationship Certificates". He stressed too that the security requirements of different sectors using the smartcard – like health and social security – are different.
- Current Internet statistics from China: 90 million users now, 50 million of which connect by dial-up and 40 million by broadband.
- Debate about Bridge CAs appears to be ongoing and no agreed model seems to have yet been reached. As reported at the last APKIF quarterly meeting, Chinese Taipei has decided to adopt Trust Lists instead of a BCA for interoperability. On the company visit in Beijing, we heard a senior private sector PKI executive state that there is no current business need for a Bridge, and that the need was at least three years away (if indeed there is ever a need). And yet a Bridge is envisaged in many government depictions, as a means to bring the many provincial government CAs together. **This might be a good topic for debate within the PKI TC.**

- Dr Hsai, Chair of the Chinese Taipei PKI Forum gave an impromptu response to my presentation on Relationship Certificates, in which he expressed some frustration with the "conservative" nature of traditional PKI, and a desire for PKI to learn more from the fast moving ICT sector at large.

Company Visits 2nd November

China iTRUS

iTRUS is one of eight certified CAs in China, and a member of the Verisign Global Trust Network (and it may be the only non government CA so certified). We were given a tour of their operations centre and a presentation on their business. The centre appears to be built in line with international CA norms, with nested physically secure zones, seven deep. Fingerprint plus proximity card is needed to enter the third and fourth tiers; the seventh zone requires two person access control. CA key generation involves the participation seven staff members, each of whom has been background-checked.

iTRUS claim to have issued around 100,000 certificates, mainly to enterprises, but also to individuals for secure e-mail and for code signing. Apparently over 90% of certificates to date have been issued to hard drives; "several thousand" have been issued to USB keys. Their offering also includes professional services, application planning, training, and "PKI products".

The start-up investment for iTRUS was around US$6,000,000.

Jilin University IT (JIT)

Jilin is a province in the North East. JIT is a commercial spin-off of a major university there, with over 200 employees, specialising in cryptographic products. Their range includes substantial hardware security modules, a variety of USB keys, and application software for enterprise security and identity management. They have also acquired three established provincial CAs The company's Chairman is very entrepreneurial and openly canvassed we visitors for our potential interest in importing JIT products or employing JIT's managed security services.

Attachments

Available in the OASIS PKI TC Members Area are the following attachments to this trip report:

— Asia PKI Forum WWCWG *PKI Business Case Book*

— Asia PKI Forum LIWG Request Form for *Legal Issues on New Security Technologies*

— Stephen Wilson presentation to the WWCWG, *The OASIS Third International PKI Survey*

— Stephen Wilson presentation to the APKIF 5th International Symposium *Relationship Certificates for Known Customers – A New Paradigm* (annotated version)

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, 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 2006 schedule of meetings is not yet complete. Confirmed so far are Korea (Inchin) for March and Taipei for November.