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

Asia PKI Forum Q2 Members Quarterly Meetings
Taipei September 2005
Trip Report for OASIS PKI TC

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

September 2005

Executive summary

The second quarterly Steering Committee and Working Group meetings for FY2005[1] of the Asia PKI Forum were held in Taipei over September 13-14. A major international PKI conference followed on September 15.

The APKIF international liaisons have expanded to include now Europe and the new Africa-Middle East PKI Forum.

My main activity on behalf of OASIS was to brief the APKIF on our international survey plans, with the aim of garnering support under the heading of Worldwide Collaboration. The Asia PKI Forum itself has yet to agree on the priorities and budget allocation for survey work. However, the PKI Forum of Chinese Taipei has begun work on its own large scale survey of 40 or more PKI "show case" organisations, with assistance from universities there, and they appear keen to collaborate on the OASIS survey.

Strong support for the OASIS survey plan was voiced by the European delegate Dr Riccardo Genghini, chair of the ETSI Electronic Signatures & Infrastructures Technical Committee, who pledged "full support to find candidates and build momentum". In addition, valuable feedback was provided on the OASIS ROI model.

Update on APKIF Membership and Activities

General business

Observers and international guests included:

[1] Note that the financial year for the Asia PKI Forum runs, not unusually, from July to June, but they number their years according to the calendar year that starts the FY. The APKIF thus refers to the current FY as 2005.

— Riccardo Genghini representing the European Telecommunications Standards Institute (ETSI); Dr Genghini chairs ETSI's Electronic Signatures & Infrastructures Technical Committee.

— Lamia Chaffai Sghaier, Director General of the Tunisian National Digital Certification Agency, and representing the new Africa-Mid East PKI Forum.

Business Case & Applications Working Group (BC/APWG)

The Business Case Book deliverable has been carried over from the last meeting, and is planned for release now in October 2005. A second edition is expected in February 2006. I offered to canvass OASIS members for business case studies to include in the following edition of the book. A template will be made available.

Electronic Certificate of Origin (ECO) initiatives (described in my July APKIF meeting report) continue to attract attention. A detailed presentation was made by the TradeVAN on a Korea-Chinese Taipei ECO being developed under the Pan Asia E-Commerce Alliance (PAA); see General Notes below for more details. Technological issues are all solved, but the project has stalled around uncertainty about compatibility between the countries' electronic signature laws and the ECO arrangements.

Work continues on a Merchant List, with the objective of marketing PKI companies in each member country or area. The catchment will be broad, to include law and consulting firms, hardware and software vendors, as well as certificate service providers. Once completed, it will be maintained and updated one or two times annually.

Interoperability Working Group (IOG)

After its huge effort in producing the 800+ page Guidebook, the IOWG has started to consider its next project. There is strong interest in working on practical interoperability testing, but widespread appreciation that the budget requirements are beyond the WG's means. My input to the discussion was that for the past five years, as far as I know, private sector contributions to PKI related bench testing has been minimal. The international X.500 and PKI Challenges, driven at first by the European Messaging Association, might be the last time large scale collaboration was undertaken.

One action was to encourage live (but modest) demonstrations by member representatives at the quarterly WG meetings.

At this meeting, a live demo was provided by Korea of the Woori Bank certificate-based net banking services. See http://www.wooribank.com.

A presentation was also made by the Chinese Taipei Ministry of Economic Affairs (MOEA) on their government PKI; see General Notes below.

Legal Infrastructure Working Group (LIWG)

The major work "Report on CA responsibilities and Liability for Cross-Border e-Commerce" was finalised and released on July 31. This 127 page document presents a detailed Policy Mapping across seven CAs in six countries: Hong Kong China Japan, Korea (two CAs), Singapore, Chinse Taipei, and Thailand.

The next project of the LIWG is a questionnaire entitled "Legal Issues on New Security Technologies and CA's Risk Management". Feedback is requested from member countries by end October.

Worldwide Collaboration Working Group (WWCWG)

Regretfully, one of the APKIF liaison representatives to OASIS, Mr Watanabe from Japan, has had to resign due to work commitments.

The WWCWG continues to work on compiling and publishing a PKI Experts listing, from member countries. They have their own preliminary plans for a "cross organisation survey" but the WG seems not to have finalised its priorities. A major part of their budget is allocated to survey work, but WG members were asking if this should be their top priority. OASIS is still the WWCWG's primary international liaison organisation.

As usual, my main OASIS liaison work was focused in the WWCWG. Here I briefed the group in detail on our international survey plans, with the aim of garnering support. While the WWCWG has yet to agree on priorities and budget for survey work, the Chinese Taipei PKI Forum has separately begun work on its own large scale survey of 40 or more PKI "show case" organisations, with assistance from universities there. They appear keen to collaborate on the OASIS survey. The universities are brining "academic rigor" to the Chinese Taipei work, and may have an analytical framework with which to analyse the results. The OASIS project would likely benefit from these strengths.

The WWCWG asked me precisely what assistance is sought be OASIS and what benefits they might expect in return. My response focused on logistical assistance, especially in arranging and conducting face-to-face surveys at Asian conferences, and identifying survey respondents. In return I suggested that influence in the survey design, access to raw data, networking with international people, and possible access to pre-publication draft reports were all possible benefits.

I received valuable feedback on the OASIS ROI Whitepaper too. It was pointed out that the digital certificate supply chain model seemed to me missing such cost components as (1) legal and compliance costs, and (2) certificate validation or OCSP services which can be charged according to a schedule of fees separate from the certificates.

The Taipei International PKI Conference 2005

This event was held after the Asia PKI Forum meetings, and was attended by 150 or so delegates. The program (see www.pki.org.tw/pkiforum2005/Epage_02.htm) featured several notable international speakers, including Dr. Stephen Kent (co-chair of the IETF PKIX committee) and Dr. Riccardo Genghini (chair of the ETSI Electronic Signatures & Infrastructures Technical Committee).

Conference highlights for me included:

— Steve Kent delivered another one of his strong critiques of traditional "Big CA" PKI and argued against the one-size-fits-all general purpose certificate: "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." He urged people to apply PKI to control "different identities in different contexts".

  Kent questioned "why do we think that a single certificate can replace all the different credentials in our wallets?". He also remarked that "issuing credentials is expensive unless you already have an authoritative database; those organisations make good CAs as they have already done the hard work".

— Kent quipped that he "finds frightening" questions about biometrics being possibly the successor to PKI. I assumed he meant that such a question is misguided in that biometrics and PKI are not applied to exactly the same thing. Further, he might be concerned that biometrics is not as mature as PKI.

  It strikes me that the OASIS PKI TC might consider doing more to clarify the relative positions of biometrics and PKI.

— A new Domain Name-linked PKI was launched recently by APNIC (the Asia Pacific Network Information Centre, one of the five top level Internet name space regulators). Kent and Genghini both lauded this new service for its move away from identity per se, lauding it as "purely an authorization PKI".[2]

— Riccardo Genghini reported that in Italy, some 2.4 million certificates have been issued to companies, with legally sanctioned Secure Signature Creation Devices (SSCDs). These certificates are compulsory for the submission of annual reports, change of registered company details and so on. While the initial introduction was mandated and therefore resisted by many on principle, surveys today indicate strong support for online company filing and digital certificates.

[2] I am sure that many PKI traditionalists will regard "authorization PKI" as a contradiction in terms, for PKI is so often thought of as inherently an *identification* system. Personally I think the sooner we see the identification-authorization dichotomy as being arbitrary, the better.

— Genghini strongly supported Stephen Kent's views on diverse identities, adding that unique identity was usually "overkill" in PKI.

General notes

— It was reported that plans for a national Bridge CA in Chinse Taipei have been dropped. Instead, the government favours cross recognition by Trust Lists (the model preferred by the APEC eSecurity Task Group).

— In Chinese Taipei, over 10 of the banks now offer "Internet ATM" where smartcards are used from personal computers to access net banking. Simple, cable-less USB smartcard readers are widely available; some 500,000 of one model alone have been sold for around US$10 each. Bank customers are anticipated to soon have 2,000,000 smartcard readers in total. One hundred thousand POS terminals and 150,000 TV set-top boxes support smartcards.

— Most bank smartcards in Chinse Taipei support symmetric encryption only. But "second generation" smartcards now rolling out support PKI.

— It was reported that Acer shipped over 1,000,000 notebook PCs with integrated smartcard readers in about three years. Acer had apparently tried to build a smartcard service business on top of this infrastructure, but the service business struggled.

— The Chinese Taipei Government PKI oversees five CAs, including one for "natural persons" and another for public sector organisations (not including the separate Health CA dedicated to servicing the National Health Insurance smartcard and 100,000 healthcare provider certificates). Natural person certificates – with smartcards – are available and must be used for certain online government services (such as tax returns). Over 1,000,000 have been issued.

— The Pan Asia E-Commerce Alliance (PAA) comprises nine members, most of which are commercial CAs or e-commerce providerz: CIECC (China), Trade-Van (Chinese Taipei), TradeLink (Hong Kong SAR), TEDI (Japan), KTNET (Korea), TEDMEV (Macau SAR), Dagang Net (Malaysia), CrimsonLogic (Singapore), and CAT Telecom (Thailand). The PAA has pioneered sector-specific PKI cross-recognition by promulgating a uniform Certificate Policy for its members, to govern certificates used primarily in electronic trade documentation. See www.paa.net.

  The PAA has gone on to develop a comprehensive electronic documentation exchange, including a defined legal framework,[3] communication protocols and ebXML templates.

[3] This framework is presumably based on commercial law and contracts, according to information I have received previously.

— Interest levels in PKI in Asia are indicated by the VIPs in attendance at the conference and the committee dinner. They included the Deputy Mayor of Taipei, and the Vice Minister for Economic Affairs. The Vice President of the Republic of China sent a personal recorded greeting.

Attachments

Request Form: Legal Issues on New Security Technologies and CA's Risk Management

Links

http://www.pki.org.tw/pkiforum2005/Epage_01.htm.

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. 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).

The next meetings are scheduled for Beijing in November and Korea in March.