Trip Report on the
African and Arab Regional Conference on Electronic Transaction Security
Digital Signature and Public Key Infrastructure (PKI)
Tunis, Tunisia June 20, 21 & 22, 2005

Arshad Noor (arshad.noor@strongauth.com)
OASIS PKI Technical Committee

The *Agence Nationale de Certification Electronique (ANCE)* or the National Digital Certification Agency of Tunisia, hosted the African and Arab Regional Conference on Electronic Transaction Security, Digital Signature and PKI between June 20 and June 22, 2005 in Tunis, Tunisia. This report presents the observations of Arshad Noor, a representative member of the OASIS PKI Technical Committee, attending and presenting at this conference, on behalf of OASIS, at the invitation of the *ANCE*.

The 2005 PKI conference in Tunis was held to bring together representatives of various African and Middle-East nations, who oversee or have a strong interest in Public Key Infrastructure (PKI), to discuss issues of common interest. Based on a visual estimate, it was very well attended with somewhere between 100 to 150 attendees. *ANCE* intends to make a detailed list of attendees available to OASIS, along with contact information. An e-mail list is also being created by *ANCE* to permit all attendees to continue communicate with each other as a forum, post-conference.

The conference began with a one-day tutorial on the fundamentals of Public Key Infrastructure to introduce the topic to those who were new to the subject. The topics covered the fundamentals of PKI – public-key cryptography, hashing, digital signatures, encryption, etc. I attended these sessions to get used to the translators (most of the sessions were in French or Arabic - which did make it a little challenging to stay in tune with the presenter, even though the translation was sometimes, excellent), as well as gauge the level of interest and knowledge of PKI amongst the attendees. All presentations are available at the *ANCE* website, by clicking on each session link, and then clicking on the individual presentation link at: http://www.certification.tn/Conference/PKITunisia2005/agenda.htm.

The second day started with Dr. Stephen Kent, Co-Chair of the IETF-PKIX WG, presenting his keynote on how far PKI had come and where he believed it was headed. In his opinion, while it had come quite a way in the last 15 years, it still had distance to go before it could be deemed ubiquitous. Much of new development appears to be sponsored by government organizations. He believed that we were missing an opportunity by not leveraging the DNS infrastructure to deploy PKI. The keynote was followed by sessions (including mine) providing updates on where PKI stood within certain geographies of the world.

Speaking for OASIS, I provided a status on the PKI Action Plan and where we were heading in the near future with that. I also provided an update on the "Transaction PKI" project which evinced interest from members of the audience who later approached me about possibly working with OASIS on this. (More on this later).

Representatives of the Asia PKI Forum – Jaeil Lee of the Korean Information Security Agency (KISA) and Secretary General of the Korean PKI Forum - provided an exhaustive update on where they were with PKI deployments in Asia. While their presentation is available online at the above-mentioned link, Stephen Wilson – in his role as the OASIS' Asia PKI Forum coordinator - provides an equally comprehensive report on the same subject in the OASIS archives.

Dr. Riccardo Genghini, Chair of the European Telecommunications Standards Institute (ETSI) Electronic Signatures & Infrastructures (ESI) Technical Committee, presented a status on PKI in Europe. From a legal perspective, there is consensus on how electronic signatures are to be treated and how countries must implement the capability. Within Italy itself - where Dr. Genghini hails from - there are more than 2M Secure Signature Creation Devices (SSCD) issued and some government applications that use legally enforcible digital signatures. Other EU states have issued SSCD's in the tens of thousands with some government sponsored applications – but mass deployment of digital certificates in the private sector has yet to happen.

The next session focused on the legal framework of PKI in different parts of the world. Since this was an extremely difficult session to follow (legal terms compounded by translation from French/Arabic to English, with even the presentations being in French), the subtle details were lost to this author. However, I did get the impression that most nations in the geography had accorded legal status to digital signatures, and established laws to setup a government Certification Authority within each country, who in turn, may either issue end-entity digital certificates, or license other commercial subordinate CA's to operate within their country.

These sessions were followed by technical sessions on the status of OpenCA by Massimiliano Palo, its Project Manager from Italy, and on Microsoft CA services by Ronny Bjones, an Enterrpise Security Strategist from Microsoft. While there was some information on PKI in the Microsoft presentation, the rest of it appeared to be more focused around marketing their perspective on general security rather than on PKI.

The third day presented many sessions on the use of PKI within applications in African and Arab nations. This session was an eye-opener for this author, because it represented the progress that appears to have been made by other countries with respect to using digital certificates for authentication and digital signatures for message integrity & non-repudiation. Tunisia, for example, is currently using digital certificates for:

- On-line tax filing
- On-line creation of company entities
- E-commerce transactions (including mobile commerce)
- Postal services
- Clearance of financial transactions
- Student authentication at Universities

It does appear from presentations of some attendees, and in discussion with attendees at this conference, that the African nations do not want to get left behind by the "information technology revolution" as they were by the industrial revolution of the early 20th century.

A common question that emerged from the forum was how the nations could participate in the e-commerce boom that had propelled first-world nations to market leading positions. Korea was held up as an example of the success of information technology and PKI adoption within its nation (12 million certificates deployed to its citizens, which represents approximately 40% penetration, and with nearly 95% broadband access to every home). The forum made some recommendations on what actions they would like to see adopted by attending representatives that might help them achieve their goal. (The DRAFT resolution was not available at the time of writing, but is expected to be distributed to attendees through the e-mail forum that will be established).

When communicating on the OASIS Transaction-PKI project (part of the PKI Action Plan's Application Guidelines SC efforts), this author got the impression that OASIS was perceived as an "American" organization that most non-American could not participate in.

As much as possible, I tried to convince them that OASIS is an open, international organization that welcomes members from any part of the world and would be glad for participation from African and Arab nations. While I emphasized that "OASIS' door is open, and all you need to do is take the first step through that door", it would behoove OASIS to focus their marketing efforts to people in this geography, reiterating the message that OASIS would welcome their participation in helping establish international technical standards towards everybody's benefit.

This author would like to express his thanks to the *ANCE* for inviting OASIS to attend this African and Arab Regional conference in Tunis, Tunisia, and to the OASIS PKI Steering Committee for choosing this author to represent it at this conference.