

## **The management and application of PKI in corporate environments** **An eema UK Regional Interest Group meeting**

Hosted by Entrust (Europe) Ltd, Reading, UK  
Thursday, 15 March 2007

Twenty-six attendees came to eema's UK RIG in Reading this March. The key theme of the meeting was to look at the use of PKI (Public Key Infrastructure) certificates to provide secure authentication, secure data storage and communications security within and between businesses. The meeting took as its standpoint the fact that the benefits of strong PKI across many business applications outweigh the cost of the PKI infrastructure management; and that PKI is not just about securing things, it is also an enabler for new, cost-effective, efficient, business processes which were hitherto not feasible because of security risks, legislation etc. In addition, the group discussed the benefits of PKI in terms of sharing more information, more widely, more affordably, and more securely, both internally and with external business partners.

Martin Linda, Siemens plc UK, Corporate Business Technology (and Chairman of the UK RIG), gave a snapshot of eema and the benefits of membership, and outlined the agenda, following which a number of speakers presented their viewpoints and case studies for discussion.

### **PKI: real world deployments**

Ian Wills, Government Account Executive of Entrust, explained that PKI was never seen as a solution of itself but is now a key part of many major business infrastructures. For example, in healthcare, defence, land registration and other sectors PKI has been installed as a major component of the security solution, where it is implemented in a manner that is transparent to users. As Ian said, PKI is at the heart of securing collaboration and providing authentication, enabling a federated trust framework within and between government, industry and communities.

### **Interoperability and liability management in the networked economy**

John Bullard, Global Ambassador, IdenTrust, explained that IdenTrust enables secure collaboration by providing an underlying validation service between banks that involves ID management across policy, legal, operations and technology dimensions. It is a rule-set of open standards that provides a root CA for financial institutions. Liability and recourse are managed by contract, enabling multiple use of applications with the same validation scheme for financial and corporate applications, and facilitating governance and compliance.

### **Certificate validation techniques**

Jon Shamah, CoreStreet EMEA described a US DoD project called Winter Storm in which US agencies involved in crisis management used the same smartcard and common interoperable digital credentials to combat and manage critical infrastructure threats. The pilot was run in six different geographical regions with different dynamic roles to demonstrate a first responder trust model in a distributed environment. A handheld device called PIVMAN was used to validate the credentials and display privileges and CRLs, and as Jon explained, a key advantage of the PIVMAN is that it does not depend on continuous on-line communications to operate. Participants in the project had valid PKI certificate based smart identity credentials, and were required to validate those credentials with a PIN. The exercise achieved 100% validation for over 1,000 credentials. The integrity of any system relies on the registration process, and the initial validation and registration was done at a central government site with additional privileges (attributes) added locally. Keeping revocation up-to-date remains one of the challenges.

### **Digital signature applications, benefits and legality in the corporate environment**

Alan Liddle, Technical Director of Trustis Ltd and BCS speaker gave some examples of authentication:

- the approval of purchases in global procurement systems
- the integration of application and PKI
- TLS over SMTP (device authentication)
- the interaction of lawyers with a government system (signing/legal validity)
- NHS medical statistics records (signing and encrypting)

As Alan said, PKIs can be deployed within five weeks for soft certificates, and the standards employed are BS7799 (ISO 27001), tScheme, GAF (Government Authentication Framework), and ETSI TS 102 042. For example, the NHS scheme has one million users carrying out eight million transactions per week. It is deployed over diverse registration authorities, authenticated to GAF level 3, and enables the signing of

Adobe PDF documents. On a cautionary note, Alan advised delegates to ensure that their PKI projects are aligned with business requirements and can be integrated into applications. In addition, legal validity varies from country to country and that too has to be mapped onto business requirements.

### **The principles for establishing a genuine e-Identity**

Ian White and Patrick McKenna of Objectsoft Ltd explained that every organisation is a local Identity provider; that common problems of registration require common solutions; that legal principles govern the creation of genuine e-identities; and that an e-ID system can implement the common legal requirements (non-repudiation) and segregation of duty. In answer to the question 'how can one ID provider trust any other ID provider?' they said that trust would become implicit if all ID providers employed the same standard business processes, and that legislation does provide for this. And in order for e-collaborations between organisations to be successful, the ID representing each organisation must be assured and trusted, minimising the risk of collusion.

### **Corporate PKI deployment case studies**

Peter Harris, Senior Consultant at Shell International described learning points and experiences from Shell's secure email service – S/MIME and PKI – implementation. The service took eight months to deliver and has been running for two years. It provides a secure global email service to support those employees who are travelling and require secure communications from all over the world. The key requirements were scalability, interoperability, ease of use and lack of central support. It is now also used for collaboration with partners, customers and suppliers. Internal MS PKI is used for logon and authentication (130,000 certificates) and external (outsourced) PKI used for signing and encryption certificates. The use of outsourced PKI leveraged supplier technical expertise and environment, operational processes for CA and key management, certificate processes and policies, and legal liability limitations. Shell has developed and published a Certificate Practice Statement (CPS) and PKI disclosure statement (the legal framework) which control the use of the service by Shell and non-Shell partners.

Peter advised attendees to make sure that they identify all the risks: legal (by using PKI lawyers), technical, procedural, organisational and financial; and to pay close attention to certificate content and management.

### **Introduction to the Siemens Corporate ID card and PKI**

Siemens AG launched their internal PKI in 1999. Martin Linda, of Siemens plc UK, Corporate Business Technology, described the current, second generation Siemens AG PKI which is based on the Siemens Corporate ID smartcard with authentication/signing and encryption certificates/keys. The requirements for the two certificates are very different and Martin described the major policy differences. The ID card is also used widely for proximity building access. In fact, Siemens has introduced many different applications employing PKI under the general headings of authentication, encryption, digital signature, access control etc, and the use of one e-ID system across all these applications delivers significant business benefit.

The Siemens AG PKI incorporates both a semi-manual service delivery channel, which utilises a service ordering tool named FIONA and over 100 issuing offices worldwide, and an automated self-service delivery channel. Martin explained that the UK Region has specific issues regarding secure delivery of cards (to level 3) to over 250 locations, and this is solved by using trained, trusted agents at each site who act on behalf of the regional issuing office.

Finally he described a number of the issues and best practices that Siemens PLC experienced with their PKI deployment. To date, over 60% of the 510,000 global employees have an ID card and PKI certificates.

***The presentations from the meeting are available on the [eema website](#). Remember that you will need your user name and password to access them.***