The Results – FAQ sheet

Q1 What is Public Key Infrastructure (PKI) and why is it so important?
A1 PKI is the infrastructure that creates and manages electronic credentials, allowing the use of digital signatures and their underlying keys and certificates across the Internet. Why so important? PKI allows the business community to communicate in a secure and trusted manner, with third parties, external suppliers, other B2B eMarketplaces and consumers.

Q2 What is the problem?
A2 A lack of interoperability between vendors' products and applications. While PKI standards were being developed (and still are being developed), different vendors implemented PKI in slightly different ways. This meant that one PKI's components were not necessarily able to communicate (interoperate) with another PKI's components.

As a result, an end-user could only guarantee secure electronic transaction and information exchange either :-

a) with another organisation using exactly the same PKI from the same vendor or

b) within their own organisation only (and only if they purchase all of the above PKI components from one vendor)

This **lack of interoperability** has long been identified as an issue in the use of PKI. EEMA stepped up to face this challenge, in the form of the pki Challenge (pkiC), a project shown to be the catalyst in bringing the leaders of this technology together to solve the interoperability problem.

Q3. What is the pki Challenge?
A3. Europe's largest PKI interoperability project - which ran between January 2001 and April 2003 - in response to growing concerns over the multiplicity and interoperability of PKI products and services available. Funded by the Swiss Government and the European Commission (under the 'Information Society Technology' Programme (1998–2002)) **the aim of the project was to identify, address and overcome these issues of interoperability.**

Q4. Who led the project?
A4. A consortium that included technology vendors (Sonera SmartTrust, *Entegrity, *Entrust, Baltimore and Utimaco), service providers (Belgacom , GlobalSign, WiSekey), Academic Institutions (University of Leuven, University of Salford), consulting companies (KPMG Information Risk Management, Makra, and Security & Standards) and a User Organisation (Royal Mail).

In addition, a Virtual Directory was produced and provided by MaXware, with the Reference System developed and supplied by Utimaco Safeware. The testing infrastructure was built and run by Royal Mail.

During the project the UK Office of the e-Envoy funded the CESG (Communications Electronics Security Group) to conduct interoperability tests in order to encourage the PKI vendor and services community to move towards the provision of PKI products and services that were interoperable. The pkiC team became aware of the CESG activity in 2001 and the two projects entered a period of collaboration. There is also a liaison agreement with the PKI Forum which has been useful for information exchange.

Q5. Was the aim of identifying, addressing and overcoming interoperability issues achieved?
A5. Yes, in spite of the withdrawal of Entegrity and Entrust from the Management Consortium, the re-structuring of Utimaco Safeware, and the inclement business climate during the life of the project.

Q6. How was the aim achieved?
A6. Ten leading PKI vendors (testing participants) tested their products against a reference implementation, using a test infrastructure, within one or more of four test plans to prove eventual or instantaneous interoperability.

Q7. Who were the testing participants?
A7. Ten testing participants are listed below, each of whom executed and reported on at least a subset of the tests.

- Baltimore Technologies
- Cryptomathic
- Guardeonic Solutions
- Microsoft
- RSA Security
- Safelayer
- TC TrustCenter
- SmartTrust/Nexus
- UTI Systems
- VeriSign

(S/MIME Client Interoperability was a required precursor to any tests involving the exchange of signed and encrypted messages.)

Q8. What were the test plans?
A8. The test plans were based on the areas of interoperability identified in the first stage of the project (Jan – June 2001) and were set to prove the following:-

- Cross Certification (between peer CAs)
- Subordinate CA Certification (from a superior CA to a subordinate CA)

- Enrolment (from a client to a CA)
- Validation (of the status of a certificate by a client)

Within the test plans, the project aimed to prove interoperability in the following potential areas:-

- the ability for applications to exchange and operate with each other's certificates
- in multiple PKI scenarios, the use of cross certification and/or user trust lists
- the use of certificate revocation solutions
- the use of supporting trust services for non-repudiation such as time stamping and timed audit logs
- the use of cryptographic techniques for digital signatures and confidentiality
- the use of qualified certificates in support of qualified signatures for the Electronic Signature Directive
- the possible use of attribute certificates
- the use of smart card technologies

For the sake of cost and management control, the method chosen was to test products and services against a reference implementation as opposed to peer-to-peer testing.

Q9. What were the objectives . . . and were they met?
A9. The **main objective** was to *test the* interoperability capabilities of the selected PKI vendors' PKI products and services (testing participants) in a series of four test plans, against a reference system, and to *identify* the interoperability issues as they arose.

This objective was met. The testing participants all proved interoperability against the test plans within which they took part, with the main technical inhibitors identified. Technical problems arising as a result of vendor product anomalies were rectified by the vendors concerned, with testing then resumed as a result. General technical inhibitors identified as being a general barrier to interoperability were documented and will be communicated in a series of best-practice guidelines to be issued as part of the pki Challenge (see Q12?).

A **secondary objective** (but nevertheless a very important one) was to promote the existence of practical solutions for Secure Electronic Commerce across Europe.

This objective was met. The project achieved recognition by the European Commission and the European business community as a whole, as a project determined to prove that PKI can and will work. The sole fact of ten key security vendors using valuable time and resource to take part in the project proved the importance of this technology and its ability to enable secure electronic commerce.

Furthermore, the building of a robust reference implementation and a strong testing infrastructure is a feat in itself, and one that can be put to good use in the future for further testing.

Q10 What were the technical findings?

A10 Unearthed during the testing phase, were a number of technical problems contributing to slow the acceptance of the technology. Some of the technical issues unearthed during the testing phase include:

- *Manual Processes vs. On-line Processes*
  Automated processes are relevant to end-entity enrolment and cross-certification, yet many products may not yet fully support automated processes.

  The project recommends, therefore that the security industry should therefore address the issue of automatic enrolment by supporting at least Simple CMC.

- *Subject Key Identifier (SKI) value*
  One participant was unable to prove the trust relationship through signed e-mail. The SKI value computed by the participant CA was different to that re-computed by the reference system.

  The project recommends therefore that:

1. PKI vendors should use 160-bit key lengths for Subject Key Identifiers.
2. Standards definitions should mandate methods whenever a value needs to be calculated.
3. PKI products should be able to use both methods of calculating the value of the Subject Key Identifier when creating a cross-certificate.
4. The SKI in the cross-certificate must match the AKI in the CA Certificate.

- *Unsigned PKCS#10s*
  Enrolments from the Reference System to the Participant System (subordination of the CA) were achieved by way of pre-generated PKCS#10 request files that were posted to the website. In one case the PKCS#10s were not signed by the CAs to which the requests pertained.

  The project recommends therefore that:
  Request files (PKCS#10), for cross-certification or subordination, should always be signed by the CA so that Proof of Possession of the CA's private signing key can be carried out.

- *Components in the Distinguished Name (DN)*
  Many directory schemas did not match the specification contained in the Interoperability Test Criteria. (This was the document produced by the project, defining which areas of interoperability should be conducted.)

  It is clear that the minimum set of attributes defined within the project was not enough to accommodate the major PKI systems that are currently available. It is equally clear that some of those systems also have problems supporting that minimal list.

There are still a large number of interoperability problems caused by the structure and flexibility allowed in the Directory components, particularly, in this case, in the Distinguished Name. The issue causes problems in the real world for both certificate and CRL retrieval and needs to be addressed. It is, however, a complex problem that has no obvious solution and will require a collaborative effort by the major players in the Security Industry.

To minimise interoperability problems, the project recommends that:
All PKI systems should support the following minimum set of components in the Distinguished Name (DN):
C (country)
L (locality)
O (organisation)
OU (organisational unit)
CN (common name)
DC (domain component)

- *OCSP Signing Certificate*
  An OCSP signing certificate issued to the Reference System OCSP Server was not signed by the same CA that issued the Certificate whose status was being determined. There are three different validation response models allowed by the standard (rfc2560), although one is more widely deployed / supported.

  The project therefore recommends that:-
  PKI implementations should consolidate on one OCSP response model.

- *Encoding of basicConstraints in End Entity certificates*
  One participant's client product could not validate the End Entity certificates issued to it from the Reference System because the default encoding contained in the certificate for the basicConstraints extension was not as expected. The Reference System was altered to exclude the CA value from the basicConstraints extension in EE certificates.

  The project concluded the following:-
  The issue of not including default values is just one example of the complexity of the standards and how rules can be different even in different parts of the same standard. This needs to be looked at in detail (see Q11).

- *Access to the pkiC website*
  It was clear that PKI protocols are not yet in common use and most firewalls have to be configured to open the specific ports. Information on firewall requirements, including specific port numbers, should be readily available to PKI users.

  The project concluded the following:-
  Users need a simple, logical explanation of how to do this. This is one of the areas to be covered within the 'User' Best Practice document. (See Q14).

- *Recertification of CAs and regeneration of download PKCS#10s*

  Following the detection and fix of many of the bugs in the Reference System it was often necessary to reissue the Root certificates and the Reference System PKCS#10s, which caused delay. The selection and configuration of the profiles and protocols used by a PKI is critical.

  The project concluded the following from this:-

  The selection and configuration of the profiles and protocols used by a PKI is critical; rebuilding and recertifying a CA to correct a problem costs both time and money. Reissuing certificates to an entire community could be prohibitively expensive and could undermine an organisation's entire PKI strategy. This is something to be communicated clearly to all those involved with a PKI.

- *E-mail clients*

  It was not the purpose of the project to prove the compliance or otherwise of e-mail clients with the S/MIME standard but the difference in performance characteristics meant that an exchange of signed e-mail to prove that a trust relationship had been established was not as straight-forward as envisaged.

  The project concluded the following :-

  1. Not all e-mail clients are S/MIME-aware
  2. S/MIME version 3 has now been adopted so new deployments of e-mail clients should support both version 3 and version 2
  3. To support enrolment to any CA, e-mail clients must be capable of producing a PKCS#10 certification request file
  4. To create a trust path an e-mail client requires access to all of the certificates in the trust chain
  5. All e-mail clients should be capable of retrieving and processing CRLs
  6. Having access to the certificate store(s) on the email client, for example to install trusted root certificates, helped to solve some problems during testing. This is not always desirable for end users and depends on company security policy

- *Website issues*

  There were problems with the usability of the pkiC Interoperability Web Site with respect to the submission of PKCS#10s by the Testing Participants. The database that supported the CAs in the Reference System was very sensitive to the reuse of information in the PKCS#10s. In particular it rejected any attempt to re-use either already submitted keys or already published Distinguished Names. It was also critical that the Testing Participant specify the correct format for the PKCS#10 file at upload so that the CA would know how to process it. This last point was merely a learning curve issue but the former two points caused repeated problems.

  The project concluded the following:-

The reuse of public keys is not strictly an interoperability issue but it could cause problems, depending on the circumstances. The re-use of Public Keys is bad practice and should be avoided.

Q11. What are the main conclusions from the pki Challenge?
A11. The most important conclusion is that **cross certification between different CAs (root CA or sub CA) can be achieved** without major problems, using a manual process.

The second conclusion is that **existing standards are far too complex**. The tests carried out within the pki Challenge identified a number of areas where the existing specifications could be improved. The EU should consider a policy of more stringent profiling, with a much greater level of detail than is currently employed e.g. specifying exactly what should be contained in fields such as the subject key identifier, rather than simply saying that a field should be present.

Similarly, the problems experienced with directory services show that **more stringent requirements should be placed on directory names and DIT structures**, rather than allowing the current 'anything goes' policy, which is a major cause of interoperability problems.

Overall, the results of the pki Challenge have hopefully provided Governments, User organisations and the vendors themselves with the confidence that PKI technology can and will work as a major technology ensuring the transaction of secure communication.

Q12. What happens now?
A12. The full report is available for public viewing at www.eema.org/pki-challenge.
The conclusions and recommendations from the pki Challenge will be used as the basis for three documents to provide clear 'Best Practice' PKI guidelines for vendors, users and the industry as a whole. The first best practice document will be aimed at the user community preparing to install a PKI, the second will give recommendations to technology vendors developing PKI products, and the third will provide challenges to the industry and standards bodies. These papers will be launched at EEMA 2003 (EEMA's 16 Annual Conference – 16-18 June 2003 in Prague) and made available to the European community via the pki Challenge web site thereafter – www.eema.org/pki-challenge