

The pki Challenge

a report by

Frank Jorissen

Vice Chairman, European Forum for Electronic Business (EEMA)

The use of the Internet and Internet-based technologies, for business as well as for private use, is increasing rapidly. Nevertheless, business and consumers have been limited to only a fraction of the potential capabilities of the Internet, especially in the area of secure electronic business and messaging. This is because, regardless of how fast the Internet is growing, the lack of practical interoperability between secure electronic-commerce-enabling technologies, such as public key infrastructures (PKI), has hindered its development.

PKI is enabling the use of digital signatures and their underlying keys and certificates across the Internet. For PKI to work between different organisations, interoperability is essential between the PKI-enabled applications ('PKA') so that they can exchange information with each other securely. To realise this goal, these applications also need to interwork properly with 'back-office' PKI components, such as certification authorities (CAs), registration authorities (RAs) and directories, etc. The latter components also need to interoperate among themselves.

Users of PKA should not be restricted to obtain all PKI and PKA components from one vendor, but rather should be able to obtain a 'best of breed' mixture of components from a large variety of vendors. These will only work properly if those vendors have proven their solutions to be interoperable, through a project such as the pki Challenge.

The problem is that, while standards were being developed, they were, and sometimes still are, under-specified. Different vendors have implemented PKI in slightly different ways, resulting in a corporate end-user only being able to conduct secure transactions and exchange information:

- with organisations using the same PKI technology (and with compatible policies); or
- within their own organisation, using only one PKI technology.

This causes numerous problems and does little to enhance the development of secure electronic business.

Only by testing the actual interoperability of these slightly different implementations, preferably in a large-scale and low-threshold project such as the pki Challenge, can deficiencies be identified and resolved.

The idea for the pki Challenge came about at the end of 1998, following the European Forum for Electronic Business's (EEMA's) highly successful participation in the global World Electronic Messaging Association (WEMA) Directory Challenge in 1997, in which interoperability using X.509v3 certificates and Secure Multipurpose Internet Mail Extensions (S/MIME) was demonstrated with limited scope and scale. It was in early 1999 when EEMA submitted a detailed proposal to the Fifth Framework Program (FP5) of the European Commission (EC) for a PKI interoperability project, aimed at solving the technical PKI interoperability issues on a global scale. The project was recognised by Europa to be a significant step along the path to a solution to the business inhibitor of PKI interoperability and, as such, fell within the remit of its FP5/Information Society Technology (IST) Programme. Full EC funding for the project was granted at the end of 2000, and the pki Challenge started on 1 January 2001.

The objective of the project is to prove that PKI interoperability can and will work as far as the underlying technology is concerned. By working with PKI vendors, users, certification service providers (CSPs), consultants and academic institutions worldwide initially, the first step of the project was to define the key areas that are believed to pose issues of interoperability. Once these areas were outlined – taking into consideration the practicalities involved and the likely availability of products and services supporting related features – PKI technology vendors were invited to submit their products to be considered for testing, based on the agreed interoperability criteria. This is the current stage of progress.

The next stage will be to select up to 25 vendors who are to take part in the testing operation. These



Frank Jorissen is Vice Chairman of the European Forum for Electronic Business (EEMA) and Deputy Vice President of Business Development for the Utimaco Safeware Group. He is also Project Co-ordinator of the pki Challenge.

complex issues

clear solutions

Booz | Allen | Hamilton

delivering results that endure

organisations will be known as 'active participants'. The testing infrastructure will then be defined and built, and the testing will begin. Each active participant will test their selected product(s) remotely against a reference implementation, which will be set up and run by Consignia (previously, UK Post Office) at their offices in the UK. The PKI technology underlying the reference implementation and fulfilling the detailed standards profile selected by the pki Challenge will be open PKI X.509 (PKIX)-compliant PKI technology, which will be fine-tuned wherever necessary. After testing against the reference implementation, the active participants can choose to also participate in bilateral peer-to-peer testing against the other active participants.

Finally, the resulting inter-working PKIs will be shown through public demonstrations at EEMA 2002 in June 2002 in Amsterdam, and at Information Security Solutions Europe (ISSE) in September 2002, with the results being disseminated globally.

The pki Challenge is a large-scale project with high but realistic ambitions. On account of this, the project organisation has been planned carefully and the project is being executed precisely. Organised by EEMA, the work is divided into eight work packages (see *Figure 1*), with each being stage-managed by one or more of a 14-strong management consortium team that comprises a defined group of PKI technology vendors, CA service providers, users, consultants, universities and research institutes across Europe.

The pki Challenge consortium consists of representatives from Baltimore (PKI vendor), Belgacom (CSP), Consignia (CSP & user), EEMA (industry association), Entegriety Solutions (PKI vendor), Entrust (PKI vendor), GlobalSign (CSP), KPMG (consultants), Makra (consultants), Security & Standards (consultants), SmartTrust (PKI vendor), University of Leuven (research institution), University of Salford (research institution), Utimaco Safeware (PKI vendor) and WISeKey (CA).

It is important to remember that the pki Challenge consortium is exactly that – a group of organisations and people that have been commissioned to manage the project, in order for the 'active participants' to engage in interoperability testing subsequently. Although most of them will do so, the fact that some of the consortium are PKI vendors does not imply automatically that all of them will be chosen to enter into the pki Challenge as active participants, nor does it mean that active participation is limited only to those organisations.

Currently, 327 individuals from over 200 organisations throughout 30 countries have registered via <http://www.eema.org/pki-challenge> as an interested party. These include people from all types of organisation who are interested in contributing their thoughts to the project, for example, to help to define the interoperability criteria, or, in other cases, are simply interested in following the progress as the project unfolds, as a learning experience.

To date, some 33 PKI/PKA vendors and CSPs have expressed an interest in becoming an active participant, and, through the work that was carried out in work package 2 (see *Figure 1*) have now submitted details of the products that they wish to put forwards for consideration, and have selected the technical criteria – applications, interfaces, protocols, etc. – within the pki Challenge scope that they ideally wish to test. The interoperability testing criteria has been outlined provisionally, with the help of the potential participants and interested parties.

It has been determined that the pki Challenge will examine the practical aspects for proving interoperability in at least the following areas. (The support for certain technologies and standards – for example, IETF's mature 'PKIX' standards – being mandatory and for others – for example, time stamping and smart cards – being optional.)

- At the most basic level, the ability for applications to exchange and operate with each other's certificates, for example, vendor A's S/MIME-based secure e-mail application using certificates generated by vendor B's PKI.
- In multiple PKI scenarios, the use of cross certification, for example, domain A (using PKI 'm') and domain B (using PKI 'n') cross-certify to recognise that they agree on the suitability of each other's PKI to conduct e-business together, and to let those PKIs 'technically enable that recognition' through the use of the resulting cross-certificates in certificate validation.
- The use of certificate revocation solutions, for example, domain B has received a transaction that is signed electronically from domain A and must find out whether the certificate corresponding to the signer's key is still valid.
- The use of supporting trust services for non-repudiation such as time stamping and timed audit logs. For example, in the case of a signature that is repudiated falsely, for the relying party to be able to prove that revocation of a signing key took place after the use of that

key for signing, the exact time of signature and certificate revocation need to be established and kept. Time services are an optional requirement in the pki Challenge.

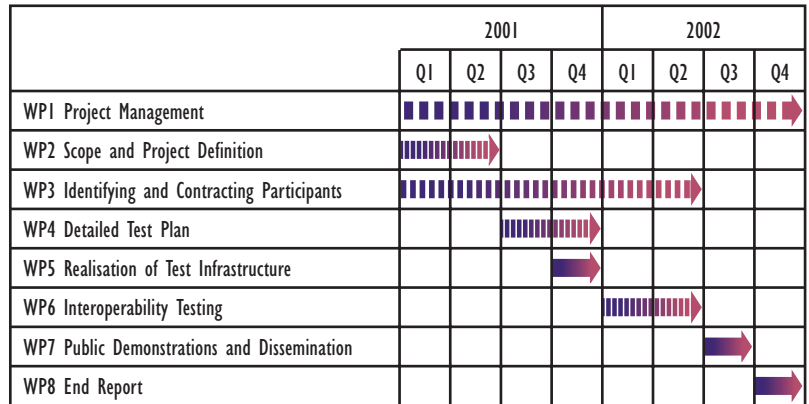
- The use of cryptographic techniques for digital signatures and confidentiality, for example, in secure e-mail.
- The use of qualified certificates in support of qualified signatures. It is a requirement to achieve equivalence of an electronic and a handwritten signature according to the European Electronic Signature Directive.
- The possible use of attribute certificates (attribute certificates are used typically to contain rather rapidly changing security parameters that are associated with a user and his or her certificate, such as access rights to corporate resources. This is an optional requirement in the pki Challenge.
- The use of smart-card technologies, for example, the use of the same smart card by similar PKA of various vendors.

The interfacing of PKI and directory systems is a special issue. Although it is not a major pki Challenge goal to be testing the interoperability of directories, directories play an extremely important role in the margin of PKI. Therefore, a realistic directory usage scenario must be covered by the project. Directories are used by both CAs and RAs to publish certificates and certificate revocation status information, for example, CRLs. In addition, they are used by PKA to retrieve this information, for example, by a signature verification application, to establish whether a signing key is still valid and, therefore, whether the signature can or cannot be relied on.

In the context of the pki Challenge, vendors will be invited to bring their favourite directory system for ‘publication’ by their CA/RA. In order to simplify things for the PKA, however, they will only need to access one ‘meta’ directory, which has been supplied kindly to the project, and set up and managed by maXware. This meta directory, when queried, will take care of all the complexities of distributing Lightweight Directory Access Protocol (LDAP) requests to the proper ‘vendor’ directory in a way that can be understood by the directory. This choice provides both an elegant and a realistic scenario.

While the pki Challenge is a discreet PKI interoperability project in its own right, all of the consortium members and active participants are very

Figure 1: Eight Work Packages of the pki Challenge



aware of the other interoperability projects that are underway.

The pki Challenge is forging formal and informal links with projects and associations such as the PKI Forum – a global, multi-vendor alliance that is very active in advancing the acceleration of interoperable PKI products and services – TeleTrust in Germany – which has set up a Bridge CA project – and the Communications Electronics Security Group (CESG) – a UK government PKI interoperability project in the UK. The list is changing constantly, as discussions continue with the associations and projects involved.

The pki Challenge is also working closely with those who are involved with the European Electronic Signature Standardization Initiative (EESSI), which is led jointly by The European Committee for Standardization (CEN) and the European Telecommunications Standards Institute (ETSI), in close collaboration with other national, European and international initiatives. EESSI is working on standardisation to meet the requirements of business within the context of the European legislative framework for electronic signatures. The pki Challenge will address the testing of qualified X.509 certificates as their standardisation by EESSI is most mature and feasible in the short term.

With the interoperability criteria definition nearing completion, and the contracting-in of the active participants underway, the future of the pki Challenge looks very promising. Its ambitious nature, strict organisational management structure and credibility within the information and communication technology (ICT) community have meant that this de facto project has gained widespread support within and outside of Europe in a relatively short space of time, as it pursues its aim to address an area of vital importance to the development of electronic business in Europe and beyond. ■