Project Descriptions

Practical Solution for Implementing a Certification Path

Security services based on digital signatures, such as RSA, require a trusted third party called key certification authority (KCA). Growing acceptance of digital signature techniques could mean a proliferation of KCAs, with adverse effect on communication between prospective partners. Extended functionality of a KCA, as described, should contain that risk.

** by Jaroslaw Tymowski*
Krajowa Izba Rozliczeniowa S.A.

The National Clearing House Co. in Poland, known also under its Polish abbreviation - KIR, operates an automated clearing house using an IT system called ELIXIR. Live production was started in April 1994 and currently about 350 bank branches (out of the population of 1700) from 20 banks can exchange payment instruments in a paperless mode. An important feature of the ELIXIR system is its safety mechanism that provides the services of entity authentication, data integrity and non-repudiation for payment instruments transfer between counterparties. This mechanism is based on the RSA public key cryptosystem. A crucial role in it is played by the Key Certification Authority (KCA). KCA established at KIR performs the following functions:

- creates the public key certificates for the users
- distributes the certificates among the users
- distributes the KCA public key.

One or Many KCAs?

As new groups of users started to prepare for implementation of a RSA-based security mechanism, as was the case in Poland, an issue was raised whether they could or should be served by the already existing KCA at KIR, or the separate KCAs should be established?

After some consideration it was agreed that even in the initial stage of development, when physical limits of any KCA platform would be no constraint to accept all interested parties, it will be beneficial to prepare for unavoidable multiplication of KCAs. Our thinking was based on the assumption that the RSA mechanism will be implemented as part of EDI development, that is among users that are more closely related between themselves (e.g. by being in the same economy sector) than with the outside world. Such groups have normally at their disposal well-proven methods of mutual identification that they do not share with other groups. Also their inclination towards specific software or hardware aspects of RSA mechanism implementation could be different from other groups. And, finally, a group could see its KCA as a centre for some additional functions, making a reconciliation of different expectations at a single KCA an impossible task.

On the other hand, it is worthwhile to maintain the benefits of the RSA mechanism, where a given user A can be authenticated through the same public key, no matter to how many users B from how many groups he is sending messages signed with his secret key. The only problem is to make sure that eventually all his counterparties have his public key certificate delivered in a secure way. In other words, it is a problem of user B trying to obtain the public key of user A, where A and B do not use the services of the same KCA to create their certificates.

Certification Path

Recommendation CCITT X.509 'The Directory - Authentication Framework' introduces a notion of a certification path that is a list of certificates needed to allow a particular user to obtain the public key of another. Each item in the list is a certificate of the KCA of the next item in the list. In a simplest case, user B would need to acquire a certificate of KCA(A) from its own KCA(B), and then a certificate of A from KCA(A). User B, knowing the public key of KCA(B) obtains the public key of KCA(A) from the first certificate, and using the public key of KCA(A) obtains the public key of A from the second certificate.

The practical problem of implementing the certification path lies in the fact that KCA(A) and KCA(B) can work in two different hardware, software and organizational environments, making it difficult and inconvenient for a user to acquire the certificates of its counterparties directly from their respective KCAs. KCA at KIR, for instance, uses smart cards to distribute its public key to the bank branches and diskettes for public key certificates (at the moment, because of the nature of ELIXIR, only one certificate is distributed, that of KIR itself). Accordingly, software implemented in the branches was designed to load KCA's public key from a smart card, and to get a public key certificate from a file. Our prospective partners from a car industry group called PLODETTE (a member of the ODETTE association) consider using diskettes for both purposes.

A straightforward implementation of the certification path would mean that a branch software should be modified to allow for extra functionality of loading a public key in a different way, but even more importantly, a processing flow at a branch would be complicated by providing two options to do basically the same thing. This is bound to cause many errors and misunderstandings, because even the basic features of the security mechanism implemented currently are creating many problems for banking staff. Taking into account that smart cards, public and secret keys, or digital signatures are all new concepts to Polish banks, and watching the difficulties people are having with PIN codes that secure the smart cards, I would not recommend going too fast with more sophisticated solutions.

Proposal

In a scheme being proposed a KCA would serve as an active intermediary for its regular users in acquiring all external certificates. On request from a user its KCA would get such a certificate from another KCA, obtain a public key of a counterparty and create its own certificate for the counterparty, signing it with its own secret key. Such a new certificate could be easily handled by the users as it would be built and delivered in a standard way for that group of users. Everything that was different in two cooperating KCAs, would be handled between the bodies better qualified to deal with any, mostly technical, complications.

An upper level could also be envisioned, a central KCA, a kind of public authority, that would certify public keys of all KCAs from a lower level and distribute a file of these certificates to all of them, together with its own public key. This would allow a KCA to verify whether a cooperating KCA is a legitimate one. The central KCA should also facilitate the establishment of a standard for exchanging certificates between KCAs.

I call the central KCA a public authority, or office, because it should be able to enforce some of its decisions on the KCAs of the lower level, that are more like voluntary associations of the users. The central KCA would decide on the approval of a new KCA as a member of the network and also on allocating a new user to an existing KCA if it cannot find one on its own. ■

**Jaroslaw Tymowski (kir_sa@vax.bpt.waw.pl) is Vice President at Krajowa Izba Rozliczeniowa S.A. in Warszawa, Poland.*