Usage of Employee-Certificates for e-Commerce

Before one commits to large-scale deployment of employee-certificates it is probably a good idea to see what applications they are actually to be used with. The following *executive-level* description highlights some of the more common applications.

1. Signed e-mail

This is the currently only widespread PKI-enabled signature-application there is. Although it certainly works, e-mail has very little to do with transaction-based systems or sophisticated inter-organization workflow, except as a notification tool. Essentially e-mail it is a person-to-person communication system.

2. Extranet login

Although employee certificates once were considered the state-of-the art solution for extranet login, recent standards like OASIS' SAML are considerably cheaper to deploy and a lot more flexible as they allow arbitrary data to be added to logins like user profiles etc. In addition, SAML reduces user-administration overhead in a way that static certificates can never do.

3. Off-line B2B

In-house e-procurement systems do currently not use individuals' identities to vouch for purchase orders (An "Our reference" field is not the same as signature), and there are few signs that this will ever be changed as "partner-IDs" seem quite logical in a B2B environment. To "filter out" employee data from certificates as many PKI-folks suggest, is a "kludge" and is likely leading to serious interoperability problems. Employee certificates also have to be revoked when an employee is no longer a part of the organization which increase costs and "fuzz". And, which person should actually vouch for outgoing purchase orders? The CEO?

4. On-line B2B

To sign orders at a market place on the web, may at first sight look like a plausible application for employee certificates. However, leading e-commerce vendors like CommerceOne, Ariba, Oracle etc. all use variations of Punchout/Roundtrip where *the uncommitted "shopping cart" is taken back to the buyer's purchasing system to be handled in the same way as any other order*. This gives control and proper internal order authorization, which buying organizations consider extremely important.

5. B2B payments

Banks usually offer outsourced payment solutions to their corporate customers. Unfortunately the currently used security solutions are all over the map, and are always defined by the banks, which eliminates employee-certificates in practically all cases.

6. Authorization

A generic problem with employee-certificates is that they do usually not certify a role etc. giving the receiving party no indication if the person is actually authorized for the transaction in progress. Using information/business systems as inter-organization communication nodes, allows authorization issues to be *handled automatically, internally, and in a considerably more trustworthy way*.

So what's left?

Essentially only internal uses. But for internal usage, an organization may choose whatever security solution they feel comfortable with. This is similar to the situation with on-line banks where all Scandinavian banks support strong authentication, while their American counter-parts only support userid/passwords. It is apparently a "cultural" issue rather than a technical ditto.

Remedy

By splitting PKI in two *independent* tracks, one supporting business unit identities (legal entity, organization etc.), and one supporting individuals (consumers), you create the foundation for *migration* to better solutions *that are aligned to current IT-architectures* but still *allow secure systems of any sophistication* to be developed. But step-wise, and based on actual needs.

V1.1 / 07-Dec-2002

Anders Rundgren
Senior Internet e-Commerce Architect
anders.rundgren@x-obi.com, +46 70 - 627 74 37