Forum of European Supervisory Authorities for Electronic Signatures (FESA)

Working Paper on Verification of Identity (Annex II section (d))

February 3, 2003

Annex II section (d) of Directive 1999/93/EC requires certification-service-providers to verify the identity of the person to which a qualified certificate is issued. According to Annex II section (d), the certification-service-provider must: “verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person”.

The clause in the Directive is fairly general and allows different interpretations in national law, which leads to a need for harmonization within EU/EFTA. The identification procedure is a critical part of the PKI and it is crucial that the correct person is identified in the certificate.

In the FESA meetings of March 7th, 2003, June 13th, 2003, and October 2nd, 2003 the interpretation of this clause was discussed and the attending members of FESA agreed, that they generally interpret this clause as described in the following text.

Note: The aim of this paper is to describe a common understanding of the interpretation of the above mentioned Annex II section (d) of the directive. It does not take into account any details of possible individual cases and of course it does not, in any way, bind the decision of a FESA member.

1. Direct or indirect identification?

Most countries have merely a general regulation that requires a direct face-to-face identification. Few countries have so far embroidered their requirements in detail, but several countries are planning to do so.

One important question is whether the regulation should allow the identity to be verified both directly and indirectly. A direct identification will imply that the person to which a qualified certificate is issued shall be identified in person face-to-face when the certificate is issued.

Indirect identification is specified by an example in the ETSI “policy requirements for certification authorities issuing qualified certificates”. The ETSI TS 101 456 section 7.3.1 c), states that:

“Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation.

NOTE 3

An example of evidence checked indirectly against a physical person is documentation presented for registration which was acquired as the result of an application requiring physical presence.”

It is likely to believe that the procedure described in the ETSI policy will be accepted by most European countries.

Generally, the identity shall be checked directly against a physical person, but for most countries it is also sufficient if the certificate holder already has been identified in person face-to-face in an existing client relationship.

Some results of the discussions:

– Who's relationship is the "existing client relationship"? (CSP / RA / associated companies). The discussion tends to the answer, that the existing client relationship of a registration authority or an associated company can be sufficient. It seems not so important who has checked the identity, but more important how the contractual relationship between the CSP and the company who has checked the identity is structured. It is the responsibility and liability of the CSP to implement a proper check of identity.

– How long ago could the direct identification have happened? Most national regulations do not have certain limits on that. The new Spanish law will allow indirect identification if the signatory has been identified not longer than five years ago or if the signatory has a notarial document.

– Some countries have more detailed requirements. Denmark has a department order which specifies § 6 of the Danish law and states that physical presence is not needed if the certification-service-provider in advance knows the person. Norway has an explicit regulation which allows indirect identification checks in § 7 of its regulation. In some countries a list of stolen id-cards is published. In Belgium it is strongly recommended to verify on this list if the id-card was stolen.

2. Copies of ID papers and revoking lists

All countries require that the identity is verified by identification papers in accordance with national law, for example by Passports, Personal ID cards, Social security ID cards or by Bank ID cards. Some countries require verification by two different identification papers. The Czech Republic has expressed that they also approve identification by a notary.

The identification procedure may require that there are made copies of the identification papers. These copies must be safely stored in accordance with national law. Having these copies enables re-identification. It might also be necessary for the certification-service-provider to have access to such copies to operate the revocation list.

The certification-service-provider is liable for the identification procedure and is usually the manager of the copied identification documents. This responsibility of the certification-service-provider is important.

3. Conclusions

The person to which a qualified certificate is issued shall be identified in person face-to-face. This personal contact is necessary. This requirement does not exclude indirect identification, i. e. use of documentation presented for registration which was acquired as the result of an application requiring physical presence, e. g. when a second certificate is required.

The certificate holder's identification papers may be copied and stored in accordance with national law to facilitate operation of the revocation list and re-identification.

The certification-service-provider is liable for the identification procedure and national law may approve evidence checked indirectly against a physical person.

It is not only important how the person is identified. In cases where the identification has taken place some time before the certificate is issued it is also important how it can be confirmed that only the person that has been identified some time ago is identical to the person that has now access to the key. Therefore the “existing client relationship” must be of a kind where the company knows if the client’s identity or name has changed since they have checked the identity.