Forum of European Supervisory Authorities for Electronic Signatures (FESA)

Working Paper on Qualified Certificates for Automatically Signing Systems

October 12, 2004

It is a frequently asked question if it is possible to use certificates of enhanced security, especially qualified certificates according to Directive 1999/93/EC, for automatically signing systems. This question is often related to the question how a signature can be created by a server on behalf of a legal person.

In the FESA meetings of October 2, 2003, February 5/6, 2004 and June 21/22, 2004 these questions were discussed and the attending members of FESA agreed, that they generally interpret the relevant clauses of the Directive as described in the following text.

Note: The aim of this paper is to describe a common understanding of the interpretation of the Directive regarding automatically signing systems. 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.

Who is the “signatory”?

Art. 2 para 3. of the Directive defines the term “signatory”: “’signatory’ means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents”.

- It is the common understanding that only a natural person can be a signatory. Neither a machine nor a legal person can be a signatory as defined by the directive.

- If a machine shall sign automatically there must always be one or more natural persons be responsible for the signatures created by the machine; one of these persons must act as a signatory.

- If a legal person wants to sign natural persons have to sign on behalf of the legal person.

Some national legislations have implemented certain exceptions of these general rules, e. g. in Austria a certification-service provider can be a “signatory” even if he is a legal person, i. e. he signs certificates and CRLs as a legal person.

Who can be the subject of a qualified certificate?

According to Annex I c) of the Directive the qualified certificate must contain “the name of the signatory or a pseudonym, which shall be identified as such”.

The wording of the Directive is technologically neutral. For qualified certificates based on X.509 the qualified certificate profile is defined in RFC 3739 which is referred to by ETSI TS 101 862.

Clause 3.1.2 of RFC 3739 describes what the subject field of a qualified X.509 certificate shall contain. The subject field shall contain an appropriate subset of the attributes: domainComponent, countryName, commonName, surname, givenName, pseudonym, serialNumber, title, organizationName, organizationalUnitName, stateOrProvinceName,

localityName and postalAddress. Of these attributes the subject field shall contain at least one of the following: commonName (choice I), givenName (choice II) or pseudonym (choice III). The organizationName and the organizationalUnitName attribute types shall, when present, be used to store the name and relevant information of an organization with which the subject is associated. The type of association between the organization and the subject is beyond the scope of RFC 3739.

Some certification-service providers use the organizationName and organizationalUnitName attributes of qualified certificates for a reference to their own organization. In this case the attributes only describe the client relationship between the signatory and the certification-service provider. But the organizationName and organizationalUnitName attributes can also be used to describe a different association between the signatory and the organization, especially that the signatory has the right to sign on behalf of the organization.

Clause 7.3.1 e) of the "Policy requirements for certification authorities issuing qualified certificates" (ETSI TS 101 456) requires:
"e) Where the subject is a person who is identified in association with a legal person, or other organizational entity, evidence shall be provided of:
– full name (including surname and given names) of the subject;
– date and place of birth, a nationally recognized identity number, or other attributes of the subject which may be used to, as far as possible, distinguish the person from others with the same name;
– full name and legal status of the associated legal person or other organizational entity;
– any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity;
– evidence that the subject is associated with the legal person or other organizational entity."

We can conclude the following from the general rule that only natural persons can be signatories and the requirements of Annex I c), of RFC 3739, and of ETSI TS 101 456:

- The signatory (who is generally a natural person) must be referred to in the subject field of the qualified X.509 certificate at least by using the attributes commonName (choice I), givenName (choice II) or pseudonym (choice III). If a pseudonym is used it must be identified as such.

- The organizationName and organizationalUnitName attributes can be used to store the name and relevant information of an organization with which the signatory is associated. The type of association between the signatory and the organization is not defined in the qualified certificate profile.

- The certificate policy or certification practice statement of the certification-service provider who issues qualified certificate shall define how the certification-service provider uses the organizationName and organizationalUnitName attributes of the qualified certificates. The certificate policy or certification practice statement shall follow the requirements of clause 7.3.1. e) of ETSI TS 101 456, especially if the organizationName and organizationalUnitName attributes do not refer to the certification-service provider itself but are used to describe a legal relationship between the signatory and the organisation.

Some national legislations have implemented certain exceptions of this general rules, e. g. in the Czech Republic qualified certificates can be issued to systems, but only for purposes of signing qualified certificates and CRLs.

Some countries use server names which are not identified as pseudonyms in the commonName attribute of the certificate.

Practical solution for automatically signing systems

An example of a practical solution for systems which sign automatically for legal persons and use qualified certificates can be described as follows:

- The certificate for the key which is used by the system is not issued to the system or to the legal person, but to a natural person who is responsible for the system – the "signatory". In the subject field either the name of this natural person is referred to in the commonName or givenName attribute or a pseudonym is used in the pseudonym attribute. In practice, it might be difficult to find a natural person who feels responsible for the system and wants to act as signatory, but this problem is independent from the use of electronic signatures. Within an organisation for each device the organisation uses there must always be at least one person responsible. The problem can be limited by using evaluated systems, because this gives the responsible person the security that the system has been tested and works properly.

- The signatory must have the mandate to sign for the legal person (the mandate can be restricted on signatures which are created by the automatically signing system). The legal person is referred to in the organizationName and/or organizationalUnitName attributes of the subject field.

- In the certificate policy and/or certification practice statement the certification-service provider describes how he uses the organizationName and organizationalUnitName attributes. The issuer can e. g. state in his certificate policy and/or certification practice statement (at least for this category of certificates) that he verifies not only the identity of the natural person, but also the identity of the legal person and that the natural person has the mandate to sign for the legal person. In this case the issuer should also state that the legal person can request certificate revocation if the natural person loses its right to sign for the legal person, and he should bind the legal person (who will typically be the subscriber for this kind of certificates) to request a revocation in this case in the contract. In this case it can be seen directly from the qualified certificate (in combination with the certificate policy and/or certification practice statement) that the signature was created on behalf of the legal person.

- A different practical solution can be, that the reference to the legal person for whom the signature is created is not included in the organizationName and organizationalUnitName attributes of the qualified certificate, but in an attribute certificate or in the signed document itself. For example, electronic bills could be signed by a provider who offers bill presentment on behalf of other organisations. In this example the commonName attribute could refer to the employee of the bill-presentment provider who is responsible for the system, the organizationName attribute could contain the bill-presentment provider's name and the signed bills could contain a reference to the company who gave the mandate to the bill-presentment provider ("This bill is signed electronically by ... on behalf of ...").

If the signatures which are created by the automatically signing system shall be advanced electronic signatures, also the following shall be noted (cf. the FESA working paper on advanced electronic signatures):

- The signatory must be able to maintain the signature-creation data under his "sole control", i. e. the system must be configured such that only the natural person who is the signatory has access to the signature-creation data.

- The signature must be uniquely linked to the signatory, i. e. the signature-creation data must be assigned only to one natural person. If the natural person who is responsible for the system is replaced by a different person, then the signature-creation data shall also

be changed and a new certificate shall be used. Changing the signature-creation data and using a new certificate is also necessary if a pseudonym is used instead of the signatories' name and the pseudonym is not changed. (According to the wording of the directive this is a requirement of the "advanced electronic signature" and not of the "qualified certificate" but the sense of the directive and many explicit requirements in national legislations also forbid that the same key pair is used by different signatories with qualified certificates.)

- If different systems sign for the same person, some require that the systems use different keys. Even if this is not required by each national legislation this can generally be seen as a best practice.

Moreover, if the signatures shall also conform to Art. 5 (1) of the Directive, a secure signature-creation device (SSCD) must be used. The typical use of Art. 5(1) signatures is a "What You See IS What You Sign" use – the signatory reads one document, enters his PIN once and creates one signature. But Annex III 2. of the Directive does not require that the signatory actually reads the document, it only requires that the SSCD must not prevent the data to be signed from being presented to the signatory prior to the signature process. This means:

- If the automatically signing system is used for batch processing, a SSCD can be used and the system can create signatures compliant to Art. 5 (1) of the Directive. In this case the signatory (the natural person being responsible for the system) must be able to see all the documents waiting in the batch to be signed before he starts the signature process. The signatory is not required to read all the documents, but he must have the possibility to read them, although he will typically only check some of the documents and maybe statistics of the whole batch before he starts the signature process, which will then sign each document waiting in the batch.

- If the automatically signing system shall sign in real-time it is typically not possible to create signatures which are compliant to Art. 5 (1) of the Directive. Nevertheless it is possible to use a qualified certificate, to create advanced electronic signatures and to use most of the security features of a SSCD. But the system will be configured in a way which prevents the signatory to see the documents before they are signed (e. g. by storing the PIN), therefore the system does not fulfil the requirement of Annex III 2. of the Directive (even if a technical device is used that would conform to Annex III if the PIN were not stored). Anyhow the signatory is responsible for the signatures which are created by the system.

- Some countries have special regulations on certain cases of automatically signing systems and give such signatures the same legal status as signatures created by SSCDs, even if the signatory cannot read the single documents before they are signed. It is seen as sufficient if the signatory knows about the general format of the signed documents and the rules which the automatically signing system will use for creating signatures after the signatory has activated it. This applies especially for time-stamping services. The requirement that the signatory is able to see the signed documents is in these cases often replaced by different security requirements (like using the key and the certificate for the dedicated purpose only, defining this in the certificate and the policy, evaluating the whole automatically signing system etc.). Some other countries have established special regulations outside the area of qualified certificates for automatically signing systems.

It is worth to note that the liability for the signatures which are created by automatically signed systems is not regulated by the electronic signature legislation but by general civil law. This especially means that – if the signatory does not sign in his own name but on

behalf of a legal person – the signatures will typically not legally bind him as a natural person but the legal person.

It is also worth to note that – even if this is not required by most legislations – companies who use automatically signing systems will typically have higher security requirements for such a system than for manually created signatures, like restricting access to the system, requiring dual control for its activation, logging procedures, or some evaluation of the software.