Forum of European Supervisory Authorities for Electronic Signatures (FESA)

Working Paper on Changes Regarding Certification-Service-Providers

October 12, 2004

In the FESA meetings on February 5 and 6, 2004 and June 21 and 22, 2004 the attending members of FESA discussed several problems about changes regarding of certification-service-providers and agreed on this working paper. Note: This paper shall just document a common understanding of these topics. It does not take into account any details of possible individual cases and of course it cannot bind the decision of a FESA member anyhow.

Introduction

Companies can be merged and split and parts of companies can be sold to other companies. It is possible that a certification-service-provider is merged into a different company, that a certification-service-provider is split into two companies or that a certification-service is sold as a whole by one company and integrated into another.

In all these cases we have to analyse if the old service and the new service are provided by the same person (i. e. if the new company has taken over all rights and duties from the old company, e. g. in the case of a merger – universal succession) or if the new company did not take over the rights and duties of the old company. It is not decisive if the two companies have agreed that the new company will stand in for the old certificates, it is decisive who is liable from the perspective of the relying party (who is typically not in any contractual relationship with the old or the new company). If the relying party has suffered damage from a wrong certificate that was issued by the “old” company it is not the relying parties duty to search for the new company who has taken over the service.

This question can be illustrated by two examples:

a) A certification-service-provider is merged into a different company. By law the incorporating company takes over all rights and duties of the company that is being merged into it. Therefore the new company becomes certification-service-provider in the moment the merger comes into effect and it automatically becomes responsible and liable for all old certificates. A relying party cannot sue the old company, because the old company does not exist as an independent legal person any more.

b) A certification-service is sold by one company to another or it is split from one company of a conglomerate and added to another. The new company does not take over all rights and duties of the company automatically; the details of the transaction are subject of a treaty. The old company continues to exist as a independent legal person. In this case the old company remains responsible for the old certificates and it remains to be a certification-service-provider. A relying party can sue the old company if a complaint is not handled properly; the relying party cannot be forced to sue the new company (especially not in the case where the new company has not enough financial capability to fulfil its claims). The supervisory authority can take supervisory measures against the old company if the remaining services (especially directory and revocation services) are not maintained properly.

Which name must be used in the issuer field?

Another topic which is related to such questions is the name used in the issuer field of qualified certificates and the names in the certification-service-provider's own certificates – especially the name in the certificate for the key that is used for signing CRLs.

According to Annex I of the Directive the qualified certificate must contain “the identification of the certification-service-provider”. As the most important purpose of the qualified certificate is identification the qualified certificate shall also properly identify its issuer.

The name used in the issuer field of a qualified certificate shall be the official name of the issuer according to the law of the state in which it is established – e. g. the name by which the issuer is registered in a trade register, but not a brand name. Cf. also Art. 5(1) a) of the E-Commerce-Directive 2000/31/EC. Technical limitations (especially the upper bound of 64 characters for the organization attribute of distinguished names, cf. “ub-organization-name” in Appendix A of RFC 3280) may require to abbreviate the official name of the issuer, but especially in conglomerates of different companies with similar names the name in the certificate shall unmistakenly identify the company who issues the certificate.

This means, that in any case where a certification-service-provider changes its name the names used in the issuer field of the issued qualified certificates must be changed accordingly. Typical technical implementations require that the key which is used for certificate-signing and the key which is used for CRL-signing also have certificates with matching names. These certificates must be changed accordingly. As it is generally seen as bad practice to use the same key in combination with different names (even in cases where the person is identical and has only changed his or her name) the certification-service-provider will typically solve this problem by setting up a new CA (which is similarly configured as the old CA) with new key pairs for certificate-signing and CRL-signing and new certificates. The old CA will be used for issuing certificates until the date of the name change, the new CA will be used afterwards.

Practical questions related to name changes

For this section it must be noted that most members of FESA have not had to decide on such questions yet and will have to evaluate them in detail according to national legislation if such a case will arise. A FESA working paper can not bind FESA members in their decisions and therefore this section can only propose how a FESA member could decide such questions:

Is it allowed that the “new CA” is set up before the name of the certification-service-provider has changed, i. e. is it allowed that a certification-service-provider uses a self-signed certificate which has been created at a point of time when the certification-service-provider whose name is in the certificate has not yet existed or has not had this name? Proposed answer: Yes (but the “new” certificates must not be used in public before the “new” provider exists or before the name has changed).

Is it allowed that the “old CA” is still used for issuing qualified certificates with the old name for certain projects? Proposed answer: No. Qualified certificates must have the real name of the issuer of the certificate in the issuer field. Relying parties must be able to work with certificates which are issued by different companies or with different issuer names.

Is it allowed that the “old CA” is still used for signing CRLs, i. e. is it allowed that the signature of a CRL is based on a certificate which contains an old and now wrong name? Proposed answer: Yes, because many technical implementations could not handle a CRL that is signed by a different key or signed by a certificate with a different name than the name in the revoked certificate. The interest of properly working signature verification is higher than

the interest of using correct names for CRL signing. – An alternative solution would be that the “old CSP” has to revoke all old certificates.

In the case where “old” and “new” certification-service-provider are different persons: Is it allowed that the “old CA” and the “new CA” use the same infrastructure; maybe even the same HSM? Proposed answer: Many countries see it as important that different certification-service-providers use different infrastructure in order to enable them to take full responsibility for their services. But in the case where a certification-service with all its infrastructure is handed over to another company it is more important that a treaty between the old and the new provider describes the responsibilities during the phase of the take-over and defines an exact time when issuing of certificates by the old CA is stopped and issuing of certificates by the new CA is started. It is not a problem, that the old CA – which is only used for maintaining the directory and CRL-signing – uses the same infrastructure as the new CA.

Is it allowed that the new certification-service uses the same key pairs for certificate-signing or CRL-signing as the old one? Proposed answer: No, because qualified certificates must be signed by an advanced electronic signature (Annex I h of the Directive) and the advanced signature must be “uniquely linked to the signatory”, i. e. the same key must not be linked to two different signatories.

Certificate renewal

It shall be noted, that a certification-service-provider has to renew his certificate not only in the case of a name change but also when the certificate expires. National legislation can have different requirements on this renewal, e. g. the following:

- that the new certificate is generated a minimum period of time before the old certificate expires,
- if the new certificate can be issued for the same key or if a new key pair must be generated,
- if or how the old and the new key pair must be cross-certified (e. g. that the new CA issues a certificate for the old key pair and vice-versa),
- if or when the old certificate will be revoked,
- if the supervisory authority maintains a national root or otherwise issues certificates to certification-service-providers it will be regulated when and under which conditions a new certificate will be issued, if the certification-service-provider has to change his key pair and if the old certificate will be revoked.