Forum of European Supervisory Authorities for Electronic Signatures (FESA)

Working Paper on Advanced Electronic Signatures

October 12, 2004

This paper is a first draft for a FESA working paper. It was discussed at the FESA meetings at February 5 and 6, 2004 and June 21 and 22, 2004.

The “advanced electronic signature” is defined in Art. 2(2) of Directive 1999/93/EC:

> 2. “advanced electronic signature” means an electronic signature which meets the following requirements:
> (a) it is uniquely linked to the signatory;
> (b) it is capable of identifying the signatory;
> (c) it is created using means that the signatory can maintain under his sole control; and
> (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

This definition differs from the signature defined in Art. 5(1) of the Directive insofar as the advanced signature is not necessarily based on a qualified certificate and not necessarily created by a secure-signature-creation device. Nevertheless the definition of the advanced electronic signature itself contains some requirements on identification of the signatory and on security.

The definition of the “advanced electronic signature” is referred to in Annex I h) of the Directive and therefore important for the supervision of qualified certificates. It is also referred to in Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax.

The definition is technology-neutral but in practice electronic signature is mostly realized by use of asymmetric cryptography and therefore the following analysis only refers to such implementations. The common use of certificates for authentication and encryption, especially via SSL/TLS (HTTPS), is not a signature according to Art. 2(1) of Directive 1999/93/EC, because it is not “attached to or logically associated with other electronic data”. Authentication occurs at initiation of the session and is not attached to the content transferred afterwards.

a) “uniquely linked to the signatory”

From this requirement it can be derived that the same key must not be assigned to different persons and that the certification-service-provider must know which key he has linked to which person.

b) “capable of identifying the signatory”

This requirement is less rigid than the requirement of Annex II d) of the Directive on qualified certificates (“verify, by appropriate means in accordance with national law, the identity”).

From this requirement the following can be derived:

1) The certificate is issued to the signatory, in most countries this is a natural person and not a legal person or a server.

2) The certification-service-provider must somehow verify the identity before issuing the certificate (but the process of verifying the identity does not need to fulfil the high requirements which apply to qualified certificates).

   Cf. ETSI TS 101 456 for qualified certificates: 7.3.1. c): “The service provider shall verify by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. 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.”

   Cf. ETSI TS 102 042 for certificates in general: 7.3.1. c): “The service provider shall collect either direct evidence, or an attestation from an appropriate and authorized source, of the identity (e.g. name) and, if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation. Verification of the subject's identity shall be by appropriate means and in accordance with national law.”

   Most countries do not have defined requirements for the verification of identity for advanced electronic signatures.

3) The use of pseudonyms in certificates that are identified as such is allowed (Annex I of the Directive allows this for qualified certificates, so it must also be allowed for advanced electronic signatures) but the certification-service-provider must know the identity of the signatory.

4) If the advanced electronic signature is created by a certification-service-provider (especially for signing qualified certificates according to Annex I h) of the Directive) the certificate on which the signature is based must identify the certification-service-provider.

c) “sole control”

Creation and storage of signature-creation data

Most requirements on the creation and storage of signature-creation data have their foundation in Annex III and Annex II j who do not apply on advanced electronic signatures. However, the advanced electronic signature must be “created using means that the signatory can maintain under his sole control”. This does not require the use of a special hardware-device as a signature-creation device, but it requires – especially in the case where the private key is stored in software – the use of security measures by the signatory to maintain his control over the key (e. g. encryption of the file which stores the private key, restriction of access to the computer and this file).

What does “sole control” mean in the context of (automatically signing) systems which are maintained by several system administrators (this is also relevant for systems that sign qualified certificates)? If the certificate is issued to a certain natural person, the security concept and the configuration of the server must ensure that only this person has control over the private key. How the person execute her control is defined in the security concept. If the certificate is issued to a legal person (which is not possible in most countries) the personnel of the legal person maintains “sole control” over the private key by its security concept.

What are the minimum requirements for the cryptographic algorithms used for advanced electronic signatures?

Most requirements on algorithms are not based on the definition of the advanced electronic signature but on the definition of the secure-signature-creation device in Annex III. From the “sole control” requirement it can be derived, that keys must not be too short, because the private key could otherwise be calculated from the public key.

It could be assumed that the requirements for algorithms used for advanced electronic signatures are weaker than the requirements derived from Annex III. Nevertheless the algorithms and parameters defined for secure-signature-creation devices are also commonly used for the advanced electronic signatures of qualified certificates (e. g. CWA 14167 refers to the ETSI SR 002 176 algo paper).

In practice users of advanced electronic signatures should have no problem to use the same algorithms and parameters, especially because advanced electronic signatures need not be created by hardware devices.

d) “linked to the data ... in such a manner that any subsequent change of the data is detectable”

This requirement can easily be fulfilled by using suitable cryptographic algorithms for hashing and signature creation.