Forum of European Supervisory Authorities for Electronic Signatures (FESA)

Important topics for the review of Directive 1999/93/EC from the supervisory authorities' point of view

June 30, 2003

According to Article 12 of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures the European Commission currently prepares a report on the review of this directive in order to submit it to the European Parliament and to the Council.

FESA, the Forum of European Supervisory Authorities for Electronic Signatures is the union of national bodies responsible for accreditation or supervision according to Articles 3(2) and 3(3) of this directive, currently comprising bodies from 12 Member States, two additional EEA EFTA States, and three Candidate Countries. Although FESA has no legal authority to impose common regulations or standards, it promotes cooperation and harmonization among its member bodies by developing common points of view, e. g. on particular issues of interpreting the Directive. This result is accomplished by regular meetings taking place at least three times a year (see http://www.fesa.rtr.at/ for details).

At the last meeting at Mainz on June 13, 2003, FESA member bodies agreed to contribute to the review process by summarizing a list of topics for the review that are important from the supervisory authorities' point of view. It is not the role of FESA to give definite proposals for changes of the Directive. But it is in the common interest of FESA members to put a light on those topics that have shown difficulties in supervisory practice. Practice has shown that some parts of the Directive are unclear and clarification would be helpful.

From the supervisory authorities' point of view the following topics are most important:

"Voluntary accreditation"

Article 3(2) gives the member states the possibility to introduce or maintain "voluntary accreditation schemes aiming at enhanced levels of certification-service provision". The member states have developed very different approaches. Some member states have established two-level schemes according to the accreditation of other products and services (the accreditation body accredits certification bodies who certify the certification-service providers). Other member states have a one-level scheme where the accreditation body (who is in some states identical to the supervisory authority) directly "accredits" the certification-service providers. Some member states did not implement an accreditation scheme at all. Also the scope of the schemes differs. Some schemes focus on qualified certificates or qualified signatures only, whereas other schemes also cover non-qualified certificates.

The use of the word "accreditation" in Article 3(2) has lead to confusion. The review process should analyse the relationship of the schemes addressed in Article 3(2) to the traditional accreditation of products and services and the wording of this provision should make clearer which schemes are intended. If the traditional accreditation is intended, this should be reflected in the wording ("accreditation", "certification"), if a different approval scheme is intended, the wording should be "approval".

In some countries voluntary accreditation or approval schemes have become the prime mechanism for establishing trust. The review should also discuss the relation between accreditation or approval schemes and supervision and possible harmonisations.

Supervision

The concept of supervision has only been touched upon by the Directive, which has lead to very different approaches in implementing supervisory schemes. Many countries have implemented a registration and a "light" check on the paperwork of the certification-service provider as part of the procedure to access the market.

Supervision differs in the amount of information to be submitted, the level of checks being performed and the question, if checks are performed by the supervisory authority itself or by an independent auditor contracted by the supervised certification-service provider. In the review process it should be analysed, if supervisory schemes shall be harmonized to create a level playing field in the EU and establish a common basis for trust or if the variety of different approaches shall be continued. Especially in the latter case information on supervisory schemes and on the status of certification-service-providers shall be made more transparent to the market place (both in a national and in a cross-border context).

Supervisors get a lot of information on internal processes and security of the certification-service provider. Stressing the need for confidentiality of this information should be a major requirement.

Depending on the national implementation of the supervisory scheme some supervisory authorities have a need to get assistance if they have to supervise a certification-service provider established on their territory, but having facilities in other countries.

"To the public"

The term "to the public" in Article 3(3) and its counterpart, the "systems, which are based on voluntary agreements under private law between a specified number of participants" in Recital 16 create a lot of confusion and are very relevant for those supervisors that have to limit their scope to those certification-service providers that issue (qualified) certificates to the public. FESA members have summarized their discussion on this topic in a working paper where we concluded, that supervisory authorities shall typically check if not only the signatories but also the relying parties are within the closed system. The review process should consider the clarification, omission or replacement of the term "to the public".

"Established"

A more precise definition of "which are established on its territory" in Article 3(3) could be helpful – especially in cases where different companies being established in different member states cooperate to provide a certification-service. This topic has also been addressed in a FESA working paper. In this paper we concluded that we will generally assume, that the certification-service provider mentioned in the issuer field of the certificate has overall responsibility and that the country where this certification-service-provider is established has responsibility for supervision.

Internal market

During the review process it should be investigated whether there are possible barriers in the cross-border recognition of electronic signatures as well as barriers in cross-border provisioning of certificate services and to what extent additional harmonisation of law and regulations are required.

Notification

Under Article 11, there is an notification requirement for those certification-service providers issuing qualified certificates to the public that have been subject to voluntary accreditation.

The review should consider the question of extending the notification requirements to other certification-service providers issuing qualified certificates to the public and the details of notification (e. g. notification of services instead of notification of providers).

We also suggest that a central list is maintained and made public of all approved secure signature-creation devices (SSCDs), of approved cryptographic modules ("trustworthy systems", Annex II, point (f)), and eventually also of other signature products. This list should also state which organisation has approved the product, based on a test from which laboratory.

All notified information concerning electronic signatures shall be made available on an European website with regular updates.

Article 3(7)

In some member states Article 3(7) has created confusion and maybe caused delays in the creation of public sector PKIs. In the review process the effects of Article 3(7) should be thoroughly analysed.

Archival of relevant data

Large differences between member states seem to exist in the "appropriate period of time" that certification-service providers are required to keep their records. The review process shall discuss if the appropriate period of time shall be harmonized or if it shall be left to national legislation.

Signature creation requirements

Annex III, paragraph 2, induced some member states to require "secure viewers" for Article 5(1) signatures, i. e. software for presenting the data to the signatory before actually signing them. Therefore, signatures created without using a secure viewer cannot be regarded equivalent to handwritten signatures in some member states. The review should clarify the requirements on signature creation. If requirements on the signature creation process are made it should also be analysed how the fulfilment of these requirements can be made visible to the relying party.

Cryptographic algorithms

On April 16, 2003 FESA has expressed in a letter to the European Commission and to ETSI, that standardized criteria on algorithms and their parameters are essential for the internal market with respect to electronic-signature products. Because of increasing computational power and growing cryptanalytic knowledge there is a demand for permanently reviewing the suitability of algorithms and parameters. In particular, mechanisms should be implemented for establishing new algorithms, for adjusting parameters, and for revoking compromised algorithms and parameters quickly.

Provision of secure signature-creation devices

Qualified signatures are created by "secure" signature-creation devices (SSCD). Annex III deals only with requirements on functions of the device. When ensuring the security of SSCDs, secure provision of the device plays important role (ref. ETSI TS 101 456). The review process should discuss requirements on the provision process of SSCDs.

Designated bodies

Article 3(4) regulates the determination of conformity for secure signature-creation devices and establishes designated bodies for this task. The conformity of the "trustworthy systems and products" in Annex II, point (f), is regulated differently and only covered by Article 3(5), although these products have great similarities. The review should consider harmonisation of the process of conformity determination for the both categories of products.

Interoperability

Interoperability is one of the important goals in the Directive to strengthen the internal market dimension of electronic signatures, but in practice interoperability problems still are one of the main obstacles.

Verification of electronic signatures

The Directive does not make clear which practice in verification of electronic signatures by relying parties is acceptable. Member states have done little in the area of implementing rules on verification. If different national rules evolve over time this could become a hindrance to the cross-border use of electronic signatures.

Relation to trust infrastructures

All practical implementations of advanced or qualified electronic signatures will be based on real world trust infrastructures. These trust infrastructures often include elements of voluntary accreditation, and therefore play a vital role in establishing the trust in (advanced) electronic signatures, besides setting a context for their practical use. To have an up-to-date overview of these trust infrastructures and their trust bases could be helpful.

Signatures of and certificates for legal persons

Although it is clear that many legal difficulties are involved it seems to be an important business need to use electronic signatures where the signatory is basically the organisation itself, especially if signatures shall be generated automatically by a server of the organisation. The review process should analyse these business needs and possible solutions and their legal and other obstacles.

Delegated signing

The market develops forms of "delegated signing" where thin end-user devices (such as mobile phones) perform the signing by relying on the signature process being carried out by a third party that also manages the keys of the end-user associated with the device. This technology opens interesting possibilities, but it also shows inconsistencies between the requirements of the definition of advanced electronic signatures, the requirements for SSCDs in Annex III, and the requirements of Annex II. It seems that the requirements of Annex III would be no problem in this case, but it is questionable whether such a scheme would meet the "sole control" requirement of the definition of advanced electronic signatures, and it is also inconsistent with the requirement in Annex II, point (j), that forbids the certification-service-provider to store the private keys.

Technology neutrality

The Directive has been set up to be technology neutral, but many regulations in the Directive link the concept of the advanced electronic signature directly to asymmetric cryptography. In the review process it should be analysed, which regulations should follow a technology-

neutral approach (e. g. Article 5(2)) and for which regulations it would be better to make the implicit link to asymmetric cryptography explicit for better understanding.

Article 9 Committee

Article 9 Committee has been largely dormant, although important interpretation issues existed and may still exist. A more active role of this committee in interpretation could be helpful. The tasks set out for the committee are defined very restrictive. A slightly more liberal definition of its tasks could be helpful.

Language issues

We want to address the possible problem, that the language in the certificate content, in associated documentation and in information supplied by supervisory authorities cannot be understood by the relying party.

Until June 30, 2003 the following FESA member bodies have approved this list of topics for the review:

Authority for IT in the Public Administration on behalf of Department for Innovation and Technologies, Italy
Federal Public Service Economy, S.M.Es., Self-employed and Energy, Belgium
Hírközlési Felügyelet, Hungary
IT- og Telestyrelsen, Denmark
Ministère de l'Économie, des Finances et de l'Industrie, France
Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), France
Ministerstvo informatiky, Czech Republic
National Post and Telecom Agency, Sweden
SWEDAC, Swedish Board for Accreditation and Conformity Assessment, Sweden
National Security Authority, Slovak Republic
National Telecommunications and Post Commission (EETT), Greece
Norwegian Post and Telecommunications Authority, Norway
Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), Netherlands
Rundfunk und Telekom Regulierungs-GmbH, Austria
Viestintävirasto, Finland

Löggildingarstofa, Iceland approved the list on July 2, 2003.