Forum of European Supervisory Authorities for Electronic Signatures (FESA)

Working Paper on “to the public” (Art. 3.3) and on closed systems (Rec. 16)

April 7th, 2003

Art. 3.3 of Directive 1999/93/EC requires member states to establish a system of supervision for certification-service-providers who issue qualified certificates “to the public”. Some countries have also a system of supervision for providers, who issue non-qualified certificates “to the public”.

According to Recital 16 of Directive 1999/93/EC, “a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised.” Such systems are mostly called “closed systems”.

In the FESA meetings of October 14th, 2002 and March 7th, 2003 the interpretation of these clauses was discussed and the attending members of FESA agreed, that they generally interpret these clauses as described in the following text. Note: This paper shall just document a common understanding of interpretation of the mentioned clauses of the directive. 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.

1. In practice the interpretation of the term “to the public” and of Recital 16 is in most cases not relevant for qualified certificates. It is therefore relevant for countries that have a supervision system for non-qualified certificates. Countries who do only supervise qualified certificates have it easier to solve this problem. Some countries generally supervise qualified certificates also if they are issued to closed user groups.

Certification-service-providers who issue qualified certificates have to invest a lot of money and are therefore generally interested in offering their certificates to as many customers as possible. And they are interested that their certificates fall under the regime of the directive and its national transformation because of the legal benefits provided by Art. 5.1. Hence qualified certificates are typically offered “to the public”.

But some countries have certification-service-providers who issue qualified certificates and construct closed systems (as they are mentioned in Recital 16). In some cases it can be economically interesting to avoid the regime of the directive but nevertheless claim to issue qualified certificates.

All those supervisory authorities who have to supervise non-qualified certificates have to deal with the interpretation of the clause “to the public” in Art. 3.3 and with Recital 16. Those supervisory authorities, who only supervise qualified certificates,

can be divided into two groups: Some of them simply supervise all issuers of qualified certificates – without taking into account if they are issued to the public or in closed systems. Others make a distinction between closed systems and issuing “to the public”.

2. If a supervisory authority has to interpret the term “to the public” and Recital 16 it typically checks if not only the signatories but also the relying parties are within the closed system.

The discussion has shown, that the interpretation is difficult and depends on the details of the individual case. But in general we define a closed system by the following elements:

- A closed system is a communication system where all participants, i. e. senders and receivers of messages, belong to a group of parties specified by voluntary agreements under private law (Recital 16). E. g. the participants belong to the same company, association, institution, etc. or the group of parties is formed by contract, statute or some other legally binding document.

- The participants of the closed system are obliged to use the certificates and the corresponding signature-creation data only within the closed system. (Some supervisory authorities demand, that the certification-service-provider has to monitor this actively.)

As an example the criteria developed by the supervisory authority of the Netherlands, OPTA, can be mentioned. OPTA defines a closed system by the following four criteria:

1. Certificates are only to be used within the group. The certificate should also state this.

2. Liability for the use of the certificate outside of the group must be restricted.

3. Contracts must restrict the use.

4. The CSP must actively do something to prevent the use outside of the group: technical means or explanations or contractual sanctions.