Forum of European Supervisory Authorities for Electronic Signatures (FESA)

Cross-border supervision of certification service providers according to member states implementation of the Directive 1999/93/EC

February 18, 2005

Introduction

The Directive allows for provision of cross-border certification services in compliance with free movement of goods and services[1] and according to article 4.1. It directs for establishment of an appropriate system of supervision of CSPs which are established on each state's territory and issue qualified certificates[2]. The supervision is usually understood as a continuous control of observation of legal requirements. Each state has somewhat different legal requirements even though the Directive contains requirements on CSP in Article 6 and Annex II and other statements.

Consequences and reasoning

This situation may have an important effect on an application of an appropriate supervision of Certification service provider that has more trustworthy systems[3] allocated in different countries. By its nature, the supervision is a privilege of an independent authority and as such is limited by constraints of the force of its legal regulation. Such a Certification service provider can not be sufficiently supervised without any further arrangements. It has been stated by the members of the FESA that this situation can be a real-life problem in the practice of national supervisory authorities; thus it is an issue.

Approach

The approach of this paper is to analyze the supervision scheme in member state countries and based on this knowledge to propose any solution. For that purpose a questionnaire has been assembled and sent to the FESA members list. Questions were primarily taken over from the Landwell's study since they were very convenient for our purposes[4]. First version of this paper was discussed on the Bratislava meeting in February 2004. Many members contributed to the discussion and brought in valuable experiences. Some changes has been done based on another discussion in Praha in June 2004. This version of the paper is based on results of the questionnaire and on results of those discussions. It may not be applicable to all supervisory authorities nor does it express opinion of all members on this issue.

---

[1] Article 10 of the Premises of the Directive
[2] Article 3.3
[3] Annex II of the Directive 1999/93/EC
[4] An attempt to gain the results of the Landwell's study itself was done but until now it was not possible to receive a proper permission.

Summary of results of the questionnaire:

Supervision is imposed on governmental body or state-organization. There is a large variety of scope of the supervision competence between every nation. There are states that supervise only CSPs that issue QC (NL, CZ, HU, DK, DE, FR, BE), but there are authorities that must supervise all CSPs that operate in its country (AT, SK, GR). There is a common statement about the limits of the supervision competence that is also supported by the FESA working paper "Established on its territory". Supervision authorities are limited by their domain boundaries which consist of real frontiers of the nation. There is also conformance between the schemes that there is no legally binding limit on the allocation of all systems of the supervised CSP. The concept of the process of the supervision is mostly very similar between members. Regularly (mostly annually, or every 3 years in systems based on ISO 17799 – DE, SE, GR) audit-like control is being conducted. It can be done by experts of the supervisory authority or by external auditors. Many states hire an auditor, who conducts the audit based on a contract. The audit control is carried out on various moments. Most of them originate from the will of the supervisory authority or they are initiated by the scheduled terms. The fact that the supervision has basic aspects of an information audit is also supported by the rights of the authority. All national authorities have rights to access all premises and documentation of supervised CSPs, may observe and investigate the running of services and may ask for full cooperation of the CSP. It is logically common for all members that the supervision liability can not be delegated. Consequences of illegal or non-compliant status or work of the CSP are also very similar. Up from the removal of accreditation or revocation of the CSPs certificate down to fees and recommendation of remedy. No responder has more experiences with cross-border supervision issue.

Results of the discussion in Bratislava

The questionnaire has shown that legislation of many member states allows for supervision that is based on audits done by third parties. Denmark, Germany, Norway and other presented that this model is being successfully practiced in their domains. France and Netherlands have prepared guidelines based on TS 101 456 for their audits. Many members contract the auditor that is also confirmed by the CSP. By this confirmation it is secured that the auditor will have permission to access premises even outside the domain of the supervisory body. Auditors need to be well selected and bust be experienced in the area of PKI.

Conclusion

Supervision schemes of member states have many common aspects such as the form of supervision control (analogy of information audits), consequences of non-compliance, nature of supervision authorities and so on. But there are also many aspects that differ national authorities from each other.
The forum discussed some solutions of cross-border supervision in Rome:

- cooperation between supervisory authorities,
- legal possibility (based on a agreement or on a legal regulation) for the supervisory authority to travel to the third country with the right to execute all necessary controls,

- delegate a third party (again based on a agreement or on a legal regulation) to execute the supervision in the third country.

Based on the discussion in Bratislava and Prague it seems to rise as a solution of the cross-border supervision:

- control of systems can be delegated and executed by third parties – auditors,
- these auditors have to have good experience and knowledge in PKI,
- they must be well selected and they should bee agreed upon by the CSP,
- such auditor can provide satisfactory control even outside of the domain of the supervision body,
- the way the auditor is chosen must be in compliance with the domain legal provision of the supervisory body (some countries require the auditor to be verified by the supervisory body, some countries leave it up to the decision of the CSP),
- concept of external auditor may be arranged by the Act or by a contract,
- possibilities of cooperation between supervisory authorities should be primarily answered question in case to case situation.