Forum of European Supervisory Authorities for Electronic Signatures (FESA)

c/o Dr. Szilveszter Ádám
Nemzeti Média- és Hírközlési Hatóság
H-1376 Budapest, Pf. 997

European Commission
DG Information Society and Media
Attn: Director-General Robert Madelin
B-1049 Brussels

Budapest, 2011-08-08

FESA statement on the planned reform of the Electronic Signature Directive

Dear Sir,

I am writing to you as the chairman of the Forum of European Supervisory Authorities for Electronic Signatures (FESA). FESA considers that the reform of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures[1] (frequently quoted as eSignature Directive) which has been initiated by the European Commission has great significance in achieving the goals set out in the Digital Agenda. In order to facilitate the revision process, I would like to present our suggestions which have been formulated drawing on the extensive in-the-field experience of our member organisations in the course of the application of the present legal framework.

Summary

FESA member bodies propose

- that transparency regarding supervision schemes, the status of supervised service providers, secure signature-creation devices and trustworthy systems should be strengthened in order to increase mutual trust;
- that the harmonisation of minimum criteria for supervision and the adoption of basic rules for cross-border supervision on the EU level should be considered;
- the terminology used in the Directive should be reviewed and definitions clarified or changed as necessary;
- improved definition of the scope and effect of “voluntary accreditation” should be considered in order to enhance the use of electronic signature services assessed under such schemes, also the relationship of such schemes to supervision should be better defined;
- increased harmonisation of conformity assessment requirements for electronic signature products should be considered;
- the Electronic-Signature Committee should play a more active role in helping the work of the Commission and

[1] OJ L 13, 19.1.2000, p. 12.

- possible barriers hindering cross-border interoperability of electronic signatures and related services should be eliminated.

Introduction

On 26th August 2010, the European Commission has published the Digital Agenda for Europe, COM(2010) 245 final/2, one of the flagship initiatives of the Europe 2020 strategy. This key document sets out the goals and charts a course to maximise the economic and social potential of ICT, most notably of the Internet and high-speed networks in improving access to content and services and in the use of innovative digital technologies. In addition to setting strategic goals and a vision for the period until 2020, the Digital Agenda also includes seven priority areas for action, one of which is "boosting internet trust and security". Connected to this priority area, two Key Actions have been determined which deal with electronic signatures and eAuthentication. Key Action 3 calls for a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems, while Key Action 16 foresees a Commission proposal for a Council and Parliament Decision to ensure mutual recognition of e-identification and eAuthentication across the EU based on online 'authentication services' offered by all Member States. The joint deadline for both key actions has been determined as the first quarter of 2012. In February 2011, the Commission has launched a public consultation on e-ID, eAuthentication and eSignature, which has generated a considerable number of responses from the stakeholders, among them also from several FESA members. The Commission has also briefed the members of FESA regularly on the state of play with regard to electronic signatures at the meetings of the organisation several times during the last few years.

FESA has always been committed to contributing to the more widespread use of electronic signatures and related services in Europe with a particular emphasis on enhancing cross-border interoperability and mutual trust. As the voice of supervisory authorities and the operators of voluntary accreditation schemes in Europe, it has contributed to these objectives through adopting and publishing a number of position papers dealing with various interpretation issues stemming from the Directive and also through participation in the dialogue with the Commission and with European Standardisation Organisations. Drawing on the extensive first-hand experience of its member organisations in the application of the national regulations transposing the Directive, FESA has identified several possible improvements that could be made in order to help the internal market of products and services related to electronic signatures develop even further. By presenting these suggestions, we hope to contribute our share to achieving the ambitious goals set out in the Digital Agenda.

1. Notifications, transparency and information-sharing

Article 3(3) of the Directive mandates that all Member States establish an appropriate system of supervision of all certification-service providers established in their territory and issuing qualified certificates to the public. However, the Directive does not contain further requirements for these supervision systems, leaving them to national implementing legislation. This has lead to many different approaches and significant variations among the supervision schemes currently in operation. Some Member States have only implemented registration and supervision schemes for service providers issuing qualified certificates, while others also register and/or supervise providers of other types of services (non-qualified certificates, time-stamping, electronic archival etc.) There are also significant differences in the amount of information required of service providers in the course of registration/supervision, in the amount and level of checks performed by the supervisory authority, including whether the checks are performed by the personnel of the supervisory

authority or by outside experts. Due to these differences, there is not enough information accessible to service providers, customers, users and relying parties about the various national registration and supervision regimes. This poses obstacles in the cross-border use and acceptance of electronic signatures and signed documents.

While supervisory authorities have a great deal of useful and valuable information about the service providers under their supervision, third parties have only limited access to even basic information related to the status of registered/supervised service providers in another country. Article 11 of the Directive only requires the notification of information related to voluntary 'accreditation schemes' and of the names and addresses of accredited service providers. This means that there is no easily accessible information available about non-accredited service providers including those that are established in a third country and benefit from the equivalence provisions in Article 7(1), although the qualified certificates issued by them have the same legal effect as those issued by providers established within the EU.

The Commission, in its Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market[2], has established a system of national Trusted Lists with the aim to increase the availability of such information. The Trusted Lists published by the Member States include standardised information in human-readable and machine-readable form about the system of supervision and about the various service providers established on the territory of the given Member State. FESA applauds the establishment of the system of Trusted Lists as a very important step in the right direction. However, we believe that further measures are necessary in order to ensure the needed transparency of registration and supervision systems and the availability of up-to-date and correct information regarding the status of service providers under supervision. In particular, we suggest the creation of a website operated and regularly updated by the Commission which includes all relevant information about the various registration and supervision systems and data about all service providers supervised by of one of the Member States or benefitting from the equivalence provisions in Article 7(1). Using Trusted Lists for this purpose may also be considered, but only if they include a human readable format which is easily accessible and readable by all interested parties, perhaps by the use of a free viewer utility or a XSL transformation file.

Additionally, we propose that the harmonisation of minimum criteria related to supervision on the EU level should be considered in a similar manner to the existing acquis (for example in Article 3 of the Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services). This step would complement the present work done in ETSI in connection with an update of the Conformity Assessment requirements and guidance under mandate from the Commission, and help strengthen mutual trust among service providers, supervisory authorities and other stakeholders on this market.

Similarly, right now there is no Europe-wide register of secure signature-creation devices assessed and certified by the various certification bodies designated pursuant to Article 3.4 of the Directive. This hinders the creation of a real single market for electronic signature products and components. Therefore FESA proposes that appropriate measures should be considered to ensure the availability of information on certified products in the EU, including an EU-wide register of such products kept and published by the Commission.

2. Cross-border cooperation in the area of supervision

[2] OJ L 274, 20.10.2009, p. 36. Commission Decision as amended by Commission Decision 2010/425/EU (OJ L 199, 31.7.2010, p. 30).

The creation of a European Single Market for electronic signature services was one of the main drivers behind the adoption of the Directive. However, in order to take maximum advantage of this single market, subscribers, signatories and relying parties need the confidence that the providers of these services operate in a trustworthy manner no matter which Member State they are established in, even if they maintain facilities in another Member State to offer services to subscribers located there. The Directive leaves open the question how such cross-border services should be supervised, and other EU legislation – most notably Art. 19 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)[3] – only deals with these issues in an indirect manner. One of the main goals behind the formation of FESA was to establish a contact network for supervisory authorities of all Member States so as to enable better information sharing and facilitate cooperation in cross-border supervision cases. However, several legal and practical obstacles have been identified that make such cooperation less practical at the present time. One of these is the fact that personnel of a supervisory authority is usually not entitled to act in an official capacity on the territory of another Member State unless that Member State has given official consent to this. Another problem is that administrative cooperation between the supervisory authorities is often made difficult by the large differences in the various national implementations of the Directive, which are reflected, inter alia, in the very different powers that supervisory authorities have in different Member States. A third problem is that most supervisory authorities are not allowed to share information collected in the course of administrative procedures due to official secrecy. Several approaches have been discussed to overcome these difficulties: One of them relies on external contracted experts that – given the consent of the service provider – can visit all facilities and access all documents regardless of the Member State they are located in, and can give an audit report to the supervisory authority in the state of establishment based on their findings. Another possible approach involves a private law agreement between the supervisory authority and the service provider giving the authority access and information rights to all facilities of the provider. Such an agreement may also be one of the conditions for joining a 'voluntary accreditation scheme' and thus bring additional benefits to the service provider concerned as well. Intergovernmental agreements between the Member States may allow personnel of the supervisory authority to act in an official capacity in another Member State, or receive appropriate administrative assistance from its counterpart. However, none of these methods may be considered as proven and sufficient at this time.

FESA members recognise that supervision is and should remain the responsibility of the Member States, but also believe that strengthening international cooperation in this area is of paramount importance for establishing trust in the cross-border use of electronic signatures and related services. Therefore we propose that the Directive should include appropriate provisions for establishing the framework of cross-border cooperation and information sharing in supervision in a similar manner to other directives which deal with the protection of the rights and interests of consumers. In this context, already established cross-border cooperation schemes, in particular the one set up under Regulation 2006/2004/EC of the European Parliament and the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation)[4] should be duly taken into account.

3. Voluntary accreditation

[3] OJ L 178, 17.7.2000, p. 1.
[4] OJ L 364, 9.12.2004, p. 1-11.

Article 3(2) of the Directive allows for the establishment of voluntary 'accreditation schemes' aiming at enhanced levels of service provision. The Directive does not further specify the scope or the operation of such schemes, but mandates that all conditions of the scheme must be objective, transparent, proportionate and non-discriminatory. According to Article 11(1), point a) all voluntary accreditation schemes must be notified to the Commission. In the more than 10 years after the adoption of the Directive, several voluntary 'accreditation schemes' have been established in the various Member States. However, these schemes follow a number of different approaches. In some Member States the scheme has two levels, with an accreditation body (either the national accreditation body, or a different organisation) accrediting the certification body or bodies which in turn certify the services. In other Member States, the scheme only consists of the certification body or bodies, which certify the services directly. Some Member States have no such schemes at all. The relation between these schemes and the supervision systems also varies.

FESA believes that voluntary schemes aimed at enhanced levels of service provision may be a very useful tool in order to further the use of electronic signatures and related services, particularly across borders. They offer a high degree of flexibility in meeting the needs of various stakeholders and as such complement mandatory national legislation. They may also contribute to the recognition of service providers that are established in third countries. However, up until now these voluntary schemes have yet to realise their full potential although in some Member States they are already playing an important role in establishing trust. In the opinion of FESA, several improvements are therefore needed. First, the use of the term 'accreditation' has led to confusion. Therefore it is suggested that the relationship between voluntary schemes described in this Directive and between accreditation and certification arrangements for other types of products and services – most notably those within the scope of Regulation 765/2008/EC of the European Parliament and the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) 339/93[5] - should be re-evaluated and clarified. If the Directive wishes to establish the same kind of two-level accreditation and certification schemes as they are also used for other types of products and services then this should be made clear in the definition and reflected in the wording throughout. Also, in this case the regulations for these schemes and general product / service accreditation and certification should be harmonised, accreditation levels for different kind of services be clearly defined, the role of national accreditation bodies be clarified. If, on the other hand, a different approach is intended then a different wording should be used to make this clear.. Secondly, the relationship between these voluntary schemes and the existing supervision systems should be analysed and possible opportunities for harmonisation should be explored.

4. Assessment of electronic signature products

The Directive and the majority of national implementing regulations as well as applicable standards define and deal with two kinds of electronic signature products. So-called 'secure signature-creation devices' (SSCDs) are defined in Article 2, point 6. The Directive contains a group of basic requirements for such devices in Annex III and calls for assessment of their conformity through designated bodies in Article 3(4). Additional requirements may be specified in generally recognised standards according to Article 3(5). In contrast, other types of 'trustworthy systems and products' are regulated differently with the only mandatory requirement contained in Annex II, point (f). The Commission may also designate 'generally recognised standards' in this area. In practice however, the two classes of products show great similarities and the required level of security for them is also similar. It is also common for designated bodies to assess the conformity of both classes of electronic signature

[5] OJ L 218, 13.8.2008, p. 30-47

products. Therefore we suggest that the extension of the scope of Article 3(4) to 'trustworthy systems and products' within the meaning of Annex II, point (f) should be considered.

Additionally, we suggest that the security requirements should also be extended to include the provisioning process for SSCDs as well as the issue of secure cryptographic algorithms, since these also play an important role in the trustworthiness of electronic signature services.

5. Internal Market and interoperability issues

One of the original aims behind the adoption of the Directive was to establish a market which would enable the free circulation of electronic signature services and products. In practice however, there are several requirements in national implementations which continue to pose obstacles in the functioning of this internal market. Such implementation requirements include the requirement to use 'secure viewers' for creating and verifying qualified electronic signatures, the requirement of 'secure PIN entry' at signature creation time as well as differing additional requirements for certain operating environments (eg: 'trusted environment' vs. 'untrusted environment') that are derived from conformity declarations/certifications. These differences in national regulations cause fragmentation in the internal market and generate insecurities among users and relying parties as to whether a qualified signature created under the regulations of one Member State is equally acceptable in another. Therefore FESA suggests that a new, revised and mandatory set of requirements be introduced into the Directive which would include all requirements that a qualified signature must fulfil in any Member State in order to be considered equivalent to a handwritten signature on a paper document. Additionally, impediments to the free exchange of electronically signed documents in a cross-border context should continue to be identified and eliminated and efforts aimed at interoperability, including standardisation, should be continued.

Similarly, there are differing national rules regarding the use of qualified electronic signatures and qualified certificates for purposes other than the declaration of intent to be bound by the contents of the document signed. Some Member States explicitly prohibit such use in their legislation, whereas others do not exclude it. In order to increase interoperability and mutual acceptance of certificates and signatures, FESA members believe it would be beneficial to include a provision regarding this use case in the revised Directive.

6. Issues with terminology

The Directive was originally intended to establish a technology-neutral legal framework for electronic signatures and related services in the EU. Therefore many of its key terms are on a very high level of abstraction, posing interpretation problems in the course of their application. FESA has adopted and published several working documents for the use of its members and the general public in the course of the years in order to help alleviate these issues, but we believe that the review of the Directive would be a good opportunity to re-assess and eliminate such interpretation issues. In the following, we present several of these unclear terms and suggest possible interpretations for them.

Article 3(3) obligates the Member States to establish a supervision system for certification service providers issuing qualified certificates to the public which are **established on their territory**. The Directive itself gives no additional guidance as to what constitutes 'establishment', which may give rise to conflicts between supervisory authorities in different Member States in the case of a service provider having facilities and providing services in several Member States. In the case of service providers issuing certificates, FESA members have adopted the common position that the service provider shall be deemed to be established in the country of its seat or residence (depending on whether the service provider

is a legal or a physical entity). This shall also be the country whose two-letter country code according to ISO 3166 appears in the “Issuer” field of the certificate. Accordingly, this is the country whose national law should apply to this service provider and which is responsible for its supervision. With other types of services, however, it is not so easy to decide on the issue of establishment. The Directive's provisions must be clear which operations are under the supervision of the "home country" and which operations are subject to supervision of the host Member State. In the case of natural persons the place of residence could be taken into account, whereas for companies the country of incorporation or formation could be used. However, it would be beneficial if the interpretation of this term could be clarified or a different term used instead.

A second key term in Article 3(3) is the issuing of certificates **to the public**. Again, the Directive does not further define the meaning of this term, which may give rise to uncertainties both among service providers and supervisory authorities, since many national implementations have followed the rules of the Directive by excluding so-called ‘closed systems’ from supervision. When it comes to making a distinction, it may be uncertain what constitutes such a ‘closed system’. FESA members have adopted the common position based on Recital 16 that in order for a system to fall into this category, it is necessary to enumerate all users of it, and examine whether they all belong to the same closed group. This includes not just the signatories and the subscribers of the eSignature service but also the relying parties. Clues indicating such a closed system may be the limitation of the use of certificates to transactions within the closed group via administrative and/or technical means, or the limitation of liability to only include such transactions. However, we are of the opinion that a clear definition of this term or the use of a different term should be considered here as well.

Annex II, point d) requires that service providers issuing qualified certificates to the public must 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. However, the Directive does not give any further guidance as to which methods are acceptable for such **verification of the identity of the applicant**. ETSI TS 101 456 requires that a service provider performs this check directly against a physical person present, but indirect methods may also be used provided they provide equal assurance to physical presence. This has lead to differing approaches and regulations in this area: some Member States strictly require that the applicant be physically present for registration, while others allow also other methods. In practice, this may mean that a bank may issue a qualified certificate to one of its clients also without the client being physically present for registration, since the client has already been identified previously (eg when opening a bank account). However, the use of indirect methods poses several important questions, including the issue of liability of the service provider for the accuracy of the data included in a qualified certificate in such cases, or the question whether it is sufficient to use only copies of official ID documents for registration. Therefore, FESA members are of the opinion that harmonisation of the most important requirements for the verification of the identity of the applicant are necessary.

Annex II, point i) requires that service providers issuing qualified certificates to the public must record and keep all relevant information concerning a qualified certificate **for an appropriate period of time**. In practice, national implementations differ widely in the length of time they specify for such records to be kept. Some Member States do not specify an exact length of time at all, others require service providers to keep these records for several decades. In the face of such big differences, FESA members suggest that it should be considered whether the length of this time should be harmonised or continue to be left to national legislation.

7. The role of the Electronic-Signature Committee

This Committee has been established by the Directive in order to assist the Commission in the fulfilment of its tasks. However, its mandate has been kept rather narrow: it may be involved in the clarification of the requirements contained in the Annexes to the Directive, in establishing criteria for bodies designated under Article 3(4) and in determining which standards the Commission should designate as 'generally recognised' pursuant to Article 3(5). This, along with a low level of activity in these areas has led to the fact that the Committee has not even had a meeting for several years. At the same time, the mandate of the Committee does not extend to many of the current and important issues that we are faced with today; involvement in the ongoing review of the Directive and in the other Key Actions connected to electronic signatures in the Digital Agenda are just examples. Therefore FESA members propose that the mandate of the Committee should be broadened, so that it could give its opinion on all issues connected to the interpretation and application of the Directive.

Conclusion

FESA members believe that the eSignature Directive has served and will continue to serve as an appropriate framework for the use of electronic signatures and related services in the European Union. The changes proposed in this document will hopefully contribute to the development of a true European Single Market for electronic signature services and products. This in turn will serve to establish mutual trust and thus facilitate the acceptance of electronic signatures and signed documents across borders.

Sincerely,

Dr. Szilveszter Ádám
Chairman