



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 15.3.2006
COM(2006) 120 final

**REPORT FROM THE COMMISSION
TO THE EUROPEAN PARLIAMENT AND THE COUNCIL**

**Report on the operation of Directive 1999/93/EC on a Community framework for
electronic signatures**

TABLE OF CONTENTS

1.	Introduction	3
2.	The Directive.....	3
2.1.	Background	3
2.2.	Implementation of the Directive	4
2.3.	Content of the Directive	4
2.3.1	Aim and scope.....	4
2.3.2.	The various types of electronic signatures in the Directive	4
2.3.3.	Internal market issues.....	5
2.3.4	Legal recognition	5
3.	Effect of the Directive on the Internal Market	5
3.1.	General remarks on the relationship between the Directive and market development	5
3.2.	The market for electronic certificates: applications in use.....	6
3.3.	Technological developments.....	6
3.3.1.	Standardisation	6
3.3.2.	Technological challenges	7
4.	The impact of Directive on other regulation	8
4.1.	The Directive 2001/115/EC	8
4.2.	The new Public Procurement Directives.....	8
4.3	The Commission Decision on electronic and digitised documents	9
5.	Conclusions	9
5.1.	The legal aspect.....	9
5.2.	The effect on the market	10

**REPORT FROM THE COMMISSION
TO THE EUROPEAN PARLIAMENT AND THE COUNCIL**

**Report on the operation of Directive 1999/93/EC on a Community framework for
electronic signatures**

(Text with EEA relevance)

1. INTRODUCTION

This Report reviews the operation of Directive 1999/93/EC on a Community framework for electronic signatures¹ (the Directive) in accordance with Article 12 of the Directive. The Report is partly based on the results of an independent study carried out by external consultants² (hereafter referred to as the Study) and finalised in 2003, and on the outcome of informal consultations with interested parties³.

2. THE DIRECTIVE

2.1. Background

Further to the first announcement of a proposal for legislation in the area of electronic signatures in a Communication on “*Security and Trust in electronic communication – Towards a European framework for encryption and digital signatures*”⁴, the proposal for a directive itself was published in 1998⁵. Several Member States had already introduced or proposed national electronic signature legislation, which they considered as a prerequisite for the growth of electronic commerce and an important policy requirement to ensure trust in electronic transactions.

From an EU perspective, national legislation with differing requirements risked holding back the effective establishment of the internal market especially in areas which depended on electronic signature related products and services. Avoiding disruption of the internal market in an area considered critical to the future of electronic transactions in the European economy was at the basis of the proposed harmonisation measures. One of the central requirements was the need to clarify the legal status of electronic signatures in order to ensure their legal validity, which was often questioned.

The Directive was adopted by the European Parliament and the Council in December 1999.

¹ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.1.2000, p.12.

² Study on the legal and market aspects of electronic signatures, K.U.L., 2003, http://europa.eu.int/information_society/eeurope/2005/all_about/trust/electronic_sig_report.pdf

³ In 2003 the Commission launched an informal consultation for all the interested parties to collect comments on the operation of the Directive. The comments received are integrated in this report.

⁴ COM(97) 503 of 8 October 1997.

⁵ OJ C 325, 23.10.1998, p.5.

2.2. Implementation of the Directive

All 25 EU Member States have now implemented the general principles of the Directive. The comments below are based on a comprehensive review of the results of the consultation and of the Member States implementing measures, though a formal analysis of the legislation transposing the Directive has not been completed at the time of this Report.

2.3. Content of the Directive

2.3.1 *Aim and scope*

The main objective of the Directive is to create a Community framework for the use of electronic signatures, allowing the free flow of electronic signature products and services cross border, and ensuring a basic legal recognition of electronic signatures.

It should be stressed that the Directive does not address the conclusion and validity of contracts or other legal obligations prescribed by national or Community law regarding the form of contracts. Neither does it affect rules and limitations relating to the use of documents, provided in national or Community law.⁶ Consequently, the Directive does not affect national provisions requiring, for instance, the use of paper for certain type of contracts. Furthermore the Directive does not exclude the possibility for parties in a closed system (e.g. corporate intranet or between a service provider and its customers) to negotiate their specific terms for the use of electronic signatures within this system.

2.3.2. *The various types of electronic signatures in the Directive*

The Directive addresses three forms of electronic signatures. The first one is the simplest form of the “**electronic signature**” and is given a wide meaning. It serves to identify and authenticate data. It can be as simple as signing an e-mail message with a person’s name or using a PIN-code. To be a signature the authentication must relate to *data* and not be used as a method or technology only for *entity* authentication.

The second form of electronic signature defined in the Directive is the “**advanced electronic signature**”. This form of signature has to meet the requirements defined in Article 2.2 of the Directive. The Directive is technology neutral but in practice, this definition refers mainly to electronic signatures based on a public key infrastructure (PKI). This technology uses encryption technology to sign data, which requires a public and a private key.

Lastly there is a third form of electronic signature mentioned in Article 5.1, which the Directive did not give a term of its own, but which for the purposes of this Report will be called “qualified electronic signature”. This consists of an advanced electronic signature based on a qualified certificate and created by a secure-signature-creation device and needs to comply with the requirements in Annex I, II and III.

⁶ The elimination of legal obstacles for the conclusion of contracts by electronic means is regulated by Article 9 of the Electronic Commerce Directive (Directive 2000/31/EC, OJ L 178, p.1)

The “**signatory**” is identified in the Directive as “a person who holds the signature creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents”. Though the Directive does not state that the electronic signature has to refer to a natural person the signatory of a qualified electronic signature (article 5.1 of the Directive) can only be a natural person as this form of signature is considered as the equivalent of the handwritten signature.⁷

2.3.3. *Internal market issues*

To promote the emergence of the internal market for certification products and services and to ensure that a Certification Service Provider (CSP) established in one Member State can provide services in another Member State, Article 3 states that market access shall not be subject to prior authorisation. In order to ensure that Certification Service Providers that issue qualified certificates to the public comply with the requirements laid down in the Annexes, Member States do, however, have to establish appropriate systems for supervision. No mandatory requirements are imposed on supervision systems. Different models have been implemented by Member States, which up to now operate mainly in their country of origin and have not demonstrated to be the source of barriers. A rise in cross border certification services could however be affected by the divergences between the Member States systems.

As regards the cross-border provision of certification services in the internal market, no restriction can be imposed on certification services provided from another Member State.

2.3.4 *Legal recognition*

Article 5.2 establishes the general principle of the legal recognition of all kinds of electronic signatures established by the Directive.

It requires Member States to ensure that the qualified electronic signature (Article 5.1) is recognised as meeting the legal requirements of hand-written signatures and that it is admissible as evidence in legal proceedings in the same way as hand-written signatures are in relation to traditional documents.

Concerning the legal effect of e-signatures, there is yet no representative case law that allows for any assessment of the recognition of electronic signatures in practice.

3. EFFECT OF THE DIRECTIVE ON THE INTERNAL MARKET

3.1. General remarks on the relationship between the Directive and market development

With the adoption of the Directive, there were some expectations that this legislation would help the market for electronic signatures to take off. Generally legislation is not introduced to create market demand, nor was it in the case of the Directive. The Directive should, however,

⁷ Restricting the use of advanced electronic signatures to natural persons shows that a lot of regulators consider e-signatures to be merely electronic equivalents of traditional handwritten signatures. However, the most common use of digital signatures is exclusively to enhance message authenticity and integrity, without the aim of showing intent to sign in the traditional sense which has also been pointed out by e.g. ICC during the informal consultation.

grant greater legal security with respect to the use of electronic signatures and related services. In that respect the Directive could provide a platform of trust that would have allowed for the market to take off.

Although the Study focussed its investigations on the use of advanced or qualified electronic signatures and found a very slow take up, it showed that many other electronic signature applications had become available that use the simpler form of electronic signatures.

3.2. The market for electronic certificates: applications in use

The two dominating electronic signature applications are related to e-government and personal e-banking services. Many Member States and several other European countries have launched e-government applications or are planning to do so. A number of these e-government applications are based on the use of electronic ID cards. The electronic ID card can be used both as an identification document and to provide on-line access to public services for the citizens. In most cases these ID cards will contain the three functionalities: identification, authentication and signing.

The other major application for electronic signatures - personal e-banking - is now taking off in most EU countries. Most of the authentication systems for personal e-banking services are relying on one-time passwords (OTP) and tokens, which means the simplest form of electronic signature according to the Directive. Many e-banking applications are only using these technologies for authentication of the user but electronic signing of transactions is increasing. For corporate e-banking (business-to-business) and inter-bank clearing, it is more common to use smart cards which are considered to provide a higher level of security.

At the same time, the spectrum of services requiring a level of authentication corresponding to the simple form of electronic signature is being widened in several Members States.

3.3. Technological developments

3.3.1. Standardisation

Article 3.5 of the Directive allows the Commission to establish and publish reference numbers of “generally recognised standards”⁸ for e-signature products. As a consequence compliance with the requirements laid down in Annex II f) and in Annex III when an e-signature product meets those standards is presumed.

The Commission issued a mandate to the European Standards Organisations to carry out the standardisation work. EESSI (European Electronic Signature Standardisation Initiative, composed by members from CEN/ISSS and ETSI) was set up and produced standards for e-signature products and services.⁹

⁸ This concept refers to the requirements of technological updatedness and of acceptance by practitioners or sufficient participation of them in its development.

⁹ The list of standards produced is available on the EESSI web site
http://www.ict.etsi.org/EESSI_home.htm

In July 2003, the Commission published a Decision based on Article 3.5 of the Directive¹⁰ including references to CEN standards (CWAs) for the requirements related to the creation of qualified electronic signatures. The validity of CWAs expires after three years of their publication; however, CEN can extend their validity for another term if needed.

According to Article 3.5, other standards can also be developed and accepted by the Commission to fulfil the requirements of the Directive as long as they can be considered to be “generally recognised standards”. In general, the requirements of the Annexes can also be fulfilled by other standards than those referenced in the OJ.

It is important for the market that future standardisation work takes into account new technological developments as in the future, users will move their e-signature key from device to device in a connected world.

3.3.2. *Technological challenges*

There is no simple answer to why the market for electronic signatures has not developed faster, but the market is facing a number of technical challenges. One frequently highlighted problem that could contribute to the slow take up of advanced or qualified electronic signatures in Europe is the complexity of the PKI technology. The often stressed advantage of PKI is that this technology uses the system of the “trusted third party” which allows parties that have never met to trust each other on the internet. In many of the current applications there seems, however, to be little interest from the service providers, essentially for liability reasons, to allow their customers to use their authentication device for other services. This is probably why the use of different one-time passwords (OTPs) is still dominating the market and there is little indication of this changing in the near future.

Other factors could explain this slow take up: the lack of provisions in the Directive on criteria for electronic signature verification services to be provided by the CSP to the end user and, the lack of provisions regarding the mutual recognition between CSPs. Depending of the countries, there are various solutions to validate a certificate such as the Root CA, the Bridge CA and the Trust Status List. In the framework of cross-border eGovernment transactions, in the IDA II Programme, action on Bridge/Gateway Certification Authority¹¹ has resulted in a Bridge/Gateway CA Pilot project which has identified not only technological problems but also legal and organisational ones.

The lack of technical interoperability at national and at cross-border level causes another obstacle for the market acceptance of e-signatures. It has resulted in many “isolated” islands of e-signature applications, where certificates can only be used for one single application. EESSI has worked on common interoperability standards but most of the Member states have specified national standards in order to promote interoperability.¹²

Today, in the PKI environment, the smart card is the mostly used signature-creation-device because the smart card provides a means to store the private key securely. This technology is

¹⁰ Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45.

¹¹ The BGCA action of the IDA II Programme : <http://europa.eu.int/idabc/en/document/2318/556>

¹² For example, the ISIS-MTT specifications in Germany aim at creating technical interoperability between the e-signatures products

expensive and requires physical infrastructure investments (distribution of cards and card readers etc). There are already a number of alternatives to the smart card that can be used to store the cryptographic key securely.

Another practical reason for the reluctance to implement e-signature applications is that the **archiving** of electronically signed documents is considered too complex and uncertain. Legal obligations to keep documents for as long as over 30 years require costly and cumbersome technology and procedures to ensure readability and verification of such period of time.

4. THE IMPACT OF DIRECTIVE ON OTHER REGULATION

Even if the demand for the deployment of PKI is something that cannot be created by legislation, the Commission still sees the introduction of electronic signatures as an important tool for the development of the information society services and to encourage secure electronic commerce.

The introduction of e-signatures and reference to the Directive 1999/93/EC has been made in some recently adopted Directives and Decisions.

4.1. The Directive 2001/115/EC

The Directive 2001/115/EC¹³ recognises the possibility to send invoices electronically. In this case, the authenticity of the origin of the invoice and the integrity of its content must be guaranteed, for example by the use of advanced electronic signatures.

The function of the advanced e-signature as referred in this Directive is to ensure that technical security during the transmission and storage process is fulfilled. In fact, in the paper-environment, not all national legislations require such a document to be signed with a handwritten signature and the Directive states that Member States shall not require invoices to be signed. It can, therefore, be said that the notion of e-signature in this case refers to a technical rather than a legal concept.

4.2. The new Public Procurement Directives

The new Public Procurement Directives, which entered into force on 30 April 2004, complete the legislative framework for the use of electronic signatures in public procurement.¹⁴

Use of e-signatures is central to establishing operational e-procurement systems across the EU. E-procurement can be expected to be one of the major fields of application, especially for more advanced forms of e-signatures. E-procurement illustrates the challenges to be overcome when promoting the use of e-signatures.

¹³ Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax, OJ L 15, 17.1.2002, p.24

¹⁴ Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transports and postal services sectors, OJ L 134, 30.4.2004, p.1 and Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, OJ L 134, 30.4.2004, p.114

The new Public Procurement Directives do not define which type of e-signatures should be used in electronic tendering but leave the choice to the Member States provided it is consistent with national law implementing Directive 1999/93/EC.¹⁵ This reflects the current practice for the submission of paper offers for which EU procurement Directives do not regulate the modalities for signing and securing offers.

The fact that Member States may choose different levels of electronic signatures implies the risk that e-procurement solutions will be designed taking into account nationally developed products. This risks fragmenting the procurement market and causing barriers to the internal market for electronic signatures.

The challenge is now to implement electronic signatures across Europe for e-procurement without creating barriers to cross border trade.

The new directives are complemented by an action plan¹⁶ which sets targets and identifies possible actions for the Commission and Member States in 2005 to 2007 to ensure that e-procurement is generalised in Europe by 2010. It calls for an operational solution for e-signatures based on mutual recognition, which mustn't be different from those used in other fields of activity.

4.3 The Commission Decision on electronic and digitised documents

The Commission Decision 2004/563 on electronic and digitised documents was adopted on 7 July 2004¹⁷. This Decision amends the internal Rules of Procedure of the Commission.

This Decision determines the conditions of validity of electronic and digitised documents for the Commission's purposes. It applies to electronic documents established or received and held by the Commission and the e-signature will be used to attest the validity of electronic documents when necessary¹⁸

The Commission has drafted the implementing rules of this Decision. They contain the principles necessary for the implementation of the e-signatures technical infrastructure.

5. CONCLUSIONS

5.1. The legal aspect

The Directive has introduced legal certainty with respect to the general admissibility of electronic signatures: the need for the legal recognition of electronic signatures has been met by the transposition of the Directive into the legislation of the Member States.

¹⁵ Cf. Annex X of procurement Directive 2004/18

¹⁶ Communication from the Commission to the Council, the European Parliament, The European Economic and Social Committee and the Committee of the Regions, Action plan for the implementation of the legal framework for electronic public procurement, 14.10.2004

¹⁷ Commission Decision of 7 July 2004 amending its rule of procedure, OJ L 251, 27.7.2004, p.9

¹⁸ It can also apply, with an agreement, for bodies or entities responsible for the implementation of certain Community policies, and with the national administrations, where a procedure involves the Commission and these other entities.

Against this background the Commission considers that the objectives of the Directive have been largely fulfilled and that no clear need for its revision has emerged at this stage.

Nonetheless, given the problems of mutual recognition of e-signatures and interoperability at a general level, the Commission will organise a series of meetings with the Member States and the relevant stakeholders to address the following issues in view of considering complementary measures, where appropriate: the differences in the transposition of the Directive; the clarifications of specific articles of the Directive; the technical and standardisation aspects; interoperability problems. In this context, account will be taken of the results from the relevant activities of the Commission services.

5.2. The effect on the market

The use of qualified electronic signatures has been much less than expected and the market is not very well developed today. Today, users do not have a single electronic certificate to sign documents or transactions in the digital environment in the same way as on paper. Therefore, the internal market objective of the Directive, the free circulation of qualified electronic signatures, cannot be assessed comprehensively at this stage.

The main reason for the slow take-off of the market is economic: service providers have little incentive to develop multi-application electronic signature and prefer to offer solutions for their own services, for instance, solutions developed by the banking sector. This slows down the process of developing interoperable solutions. The lack of applications, such as comprehensive solutions for electronic archives, might also prevent the development of a multi-purpose e-signature, which requires reaching a critical mass of users and usage.

A number of applications in the future might however trigger market growth. The use of e-signatures in e-government services has already reached a certain volume and will probably be an important driver in the future. The strategic role of eGovernment applications is recognised in the i2010 initiative¹⁹, which fosters the deployment and efficient use of ICT by the private and public sectors. The need for secure electronic means of identification to access and use public services is essential for citizens and businesses and will promote the use of electronic signatures²⁰. Different forms of eID will be emerging and will require some degree of interoperability. The Commission has set a high priority on eID initiatives, through for instance, the eProcurement action plan or the harmonisation of security features of travel documents, the IDABC programme action on the interoperability aspects of eID for pan-European eGovernment services, the IST or the eTen Programmes. Internally, the Commission intends to continue the modernization of its own administration.²¹ The future deployment of e-signatures to reduce paper circulation is one of these measures.

The Commission will continue to encourage the development of e-signatures services and applications and will monitor the market. Beyond the support through eGovernment activities, particular emphasis will be on interoperability and cross-border use of electronic signatures. The Commission will encourage further standardisation work in order to promote the interoperability and use of all kinds of technologies for qualified electronic signature in the internal market. It will prepare a report on standards for electronic signatures in 2006.

¹⁹ COM(2005) 229 final

²⁰ see also the Ministerial Declaration approved unanimously in Manchester during the Ministerial e-government Conference « Transforming Public Services », 24/11/05

²¹ “e-Commission 2006-2010: enabling efficiency and transparency” - strategic framework - C/2005/44 73