Electronic Signatures Legislation in European Law. Its Use and Efficacy.

By Ingrid Havemann

A. Legislation concerning Electronic Signatures ➦

Companies saw the Internet as an instrument of public relations, until now, but it is more and more seen as an instrument of direct marketing of their products and services.

Open electronic networks such as the Internet are of increasing importance for worldwide communication. They offer the possibility of interactive communication between parties who may not have pre-established relationships. Open networks offer new business opportunities by creating tools to enhance productivity and minimize costs, as well as new methods of reaching customers. Networks are being used by companies that wish to take advantage of new ways of doing business and new means of working, such as telework, shared virtual environments, etc. To make the best use of these opportunities, a secure environment is needed with regard to electronic authentication [1] .

It is necessary to use electronic signatures to improve the safety of communications and transactions by new technologies. Electronic signatures allow addressees of electronically transmitted data to verify the origin of the data and check that they are complete and unaltered and thus preserve their integrity.

We will see which laws exist concerning digital signature. The legal sources in this matter differ worldwide. Basically: The rules of the international civil law determines which law is applicable in the individual case. Let's have a short summary of the international legal position now.

I. Which legal sources exist concerning electronic signatures? ➦

Worldwide, laws on e-signature are a recent phenomenon. Stimulated by the development of the American Bar Association Digital Signature Guidelines, electronic signature legislation began with the Utah Digital Signature Act [2] , which was enacted in 1995 and focused solely on issues raised by cryptography-based digital signatures. Soon thereafter, legislation was introduced in several other states.

Also, on October 1, 2000, the Electronic Signatures in Global and National Commerce Act ("E-SIGN Bill") became federal law in the United States, and "digital contracts" that consumers form online have the same legal status as pen-and paper contracts. In the Asian region, Japan established an E-Signature Law [3] , (Law Concerning Electronic Signatures and Certification Services) on April 1, 2001. The law's purpose is to make sure the easy use of electronic signature and prompt electronic data exchange in such as e-commerce through the Internet.

A good overview of the international legislative, the signature acts and relevant

ordinances, is presented e. g. at "www.revistasdederecho.com/firma digital" and at www.mbc.com/ecommerce/international.asp.

II. What is the European Community framework for electronic signatures? ➦

The Community's first steps towards regulating electronic signatures were taken in the Commission's 1997 Communication, "A European Initiative in Electronic Commerce", which emphasised the need for legislation [4] . and were followed by the Commission Communication , "Towards a European Framework for Digital Signatures and Encryption" [5]

.

Because of the different national legislation concerning electronic signature the communication and electronic commerce in the EU had been more complicated than necessary. In order to resolve this problem and ensure the proper functioning of the internal market in the field of electronic signatures by creating a harmonised and appropriate legal framework for the use of electronic signatures within the European Community- For that reason the European parliament together with the European Council decided to publish a Directive for Electronic Signature.

On January 19, 2000, the Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures was published [6] . The Directive had been implemented in all member states by July 19, 2001.

III. What are the essential contents of the of the Directive 1999/93/EC?

The goal of this directive [7] "lays down the criteria which form the basis for legal recognition of electronic signatures by focusing on certification services. These comprise the following:

- common obligations for certification service providers to secure trans-border recognition of signatures and certificates throughout the European Community;
- common rules on liability to ensure confidence on the part of users, on the basis of certificates, and of service providers;
- cooperative mechanisms to facilitate trans-border recognition of signatures and certificates with non-member countries.

The directive includes in its Article 2 definitions of:

- electronic signature [8] and advanced electronic signature [9] ;
- signatory;
- signature creation device;
- signature verification device;
- qualified certificate;
- certification service provider;
- electronic signature product.

Member States will not make the provision of certification services subject to prior authorisation. They may introduce or maintain voluntary accreditation schemes to enhance the level of certification service provision. All conditions relating to such schemes must be objective, transparent, proportionate and non-discriminatory."

This directive seeks to avoid excessive restrictions in national legislation. Thus the Directive includes the following rules:

“Each Member State must apply the national provisions it adopts pursuant to this directive to certification service providers established in its territory and to the services they provide. Member States may not restrict the provision of certification services that originate in another Member State in the fields covered by this directive. Member States must ensure that electronic signature products which comply with this directive are permitted to move freely on the internal market.

Member States must ensure that an electronic signature is not denied legal effect, validity and enforceability solely on the grounds that the signature is in electronic form or not based upon a qualified certificate, or upon a certificate issued by an accredited certification service provider. Member States must ensure that electronic signatures based on a qualified certificate issued by a certificate service provider which fulfils the requirements laid down in the directive are recognized as being in conformity with the legal requirements relating to handwritten signatures and are admissible as evidence in legal proceedings in the same manner as handwritten signatures.

Member States must ensure that by issuing a qualified certificate a certification service provider is liable to any person who reasonably relies on the certificate for:

- the accuracy of all information in the qualified certificate;
- compliance with all requirements of this directive in issuing the qualified certificate;
- assurance that the holder identified in the qualified certificate held, at the time of the issuance of the certificate, the signature creation device corresponding to the signature verification device given or identified in the certificate;
- in cases where the certification service provider generates the signature creation device and the signature verification device, assurance that the two devices function together in a complementary manner.

Member States must ensure mutual recognition of electronic signatures as legally equivalent. The Commission must make proposals to implement standards and international agreements applicable to certification services. With the agreement of the Council, the Commission may negotiate market access rights for Community undertakings in third countries.

Member States must ensure that certification service providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in the national provisions implementing Directives 95/46/EC and 97/66/EC.

The Commission will be assisted by an advisory committee, called the "electronic signature committee".”

The Directive is, in line with the OECD [10] and Unicitral [11] developments cited above, technology-neutral and does not focus upon any particular kind of electronic signature. Currently, the most commonly-used type of electronic signature is public-key cryptography, but there is no guarantee that this will be the case in the future.

The Directive is designed to be applicable to technologies which have not yet developed [12] .

IV. What are the legal effects of the use of digital signatures in the European Union? ➦

The Directive is intended to have wide legal effects with respect to electronic signature. Two of the most important effects are in the areas of equal recognition and liability.

Member States are obliged to ensure that an electronic signature is not denied legal effect solely on the ground that is in electronic form, and that certified electronic signatures are recognised as satisfying any legal requirement of a hand-written signature [13] . In order to promote trust the Directive establishes a basic rule that certification service providers shall be liable for their certificates to anyone who reasonably relies upon them [14] .

V. Where do I find information about LEGISLATION ON ELECTRONIC SIGNATUREs IN the MEMBER STATES? ➦

Meanwhile, in each Member State exist Digital Signature Legislation that try to bear in mind the directives criteria [15] . Some examples are the following laws [16] :

German Law [17] : The legal basis for the electronic signature is the „Signatur Gesetz [18] ." (Digital Signature Act) . Article 3 of the German Information and Communication Services Act of 22 July 1997 features the Digital Signature Act which came into force on 1 August 1997. The Digital Signature Ordinance of 22 October 1997 took effect on 1 November 1997, and is based on §16 of the Digital Signature Act. The purpose of the Act is to create an appropriate framework for the safe use of digital signatures and the reliable detection of forged signatures and manipulated signed data. The current version from 2001 (Sign2001) was introduced by the "Law about the framework conditions for electronic signatures" and convert the mentioned community legal framework conditions for electronic signatures.

Austrian Law: The basis for acknowledging electronic signatures under Austrian law was created by the Federal Electronic Signature Act (Signaturgesetz). The Signature Act is explained in more detail by the Signature Ordinance (Signaturverordnung). With the Ordinance BGBL II 20002/117 the European minimum criteria for notifying confirmation bodies were published in the Austrian official journal. The A-SIT Ordinance (BGBl II 2000/31) recognized the Secure Information Technology Center – Austria (A-SIT) as a confirmation body. The Signature Ordinance, which went into effect on February 3, 2000, gives concrete explanations of the Signature Act, especially with regard to technical matters.

United Kingdom: In British law the "Electronic Signatures Regulations 2002" from 8th March 2002 implement the Directive 1999/93/EC. Under Section 7 of the Electronic Communications Act 2000, electronic signatures or e-signatures are made legally admissible in the UK [19] .

Spanish Law: Under Spanish law electronic signatures are regulated by the Royal Decree-Law 14/1999 (Real Decreto-ley 14/1999 de 17 de septiembre sobre la firma electrónica). This is running legislation proceeding about the draft to a new signature act at present, ("Borrador de Anteproyecto Ley de Firma electrónica de 2002"). Also important is the Spanish "Law about the Services of the Information Society y the Electronic Commerce" (Ley 34/2002 de 11 de Julio de servicios de la sociedad de la information y de comercio electrónico, BOE 166, 12. Julio 2002.) Article 23 e. g. of this "LSSI" regulates the validity

and the effectiveness of electronic contracts.

B. Guide on the use and efficacy of electronic signatures. ➦

To sign a document is a simple operation in the real world. The question complicates in the virtual one: it needs the use of cryptography and codified messages. But the difficulties, which are expected, are not as complicated as it might seem on the first view. Now we will turn to the typical problems concerning electronic signatures at the example of the Spanish law [20] .

In the following are answered some of the questions frequently asked [21] .

I. Frequent Questions regarding to the use of electronic signatures. ➦

1. What do we have to understand by "electronic signature"? ➦

It is a group of data, like codes or cryptographic keys that connect one with an electronic document unequivocally. (contained in a support magnetic -diskette or hard drive of an computer,) that allows to identify to the headline who he attributes.

If this procedure being highly trustworthy and grace allowing to detect any unauthorized alternation of the document to which devices used in the creation of the signature are safety, by fulfilling certain technical exigencies and because the - certification service provider that he has supervised is "accredited", (has passed an professional exam), then it is called "advanced electronic signature".

2. How are electronic signatures used? ➦

[22] We just need a computer with access to Internet and a device card reader of electronic signature. We must attend to certification service provider, which will proceed to our personal identification next. After that it will generate our public and private keys and it will deliver us our private key. Also you have to install in your computer the software application or necessary program for use it.

With it we are ready for the signature of a document or file that we have created and can send a encrypted document directly to the addressee. At the same time he will receive a document with the certification of the service provider that permit him to identify the author.

3. Where are our electronic signatures safe? ➦

The private key is incorporated in intelligent cards, similar to credit cards. They have one chip that contains information of the author, emitted entity an the hole bits of the key. These cards are protected by a secret code which only the holder knows, that’s why these are personal and untransferable.

4. What is the legal value of an electronic signature? ➦

The "advanced electronic signature" has in relation with an electronic document the same legal value as the handwritten signature in relation with an paper.

It its obligatory his admittance as a proof in a trial. The proof must be valued in keeping with the criteria of judicial appreciation established in the procedural rules.

If one against whom, he imputes an electronically signed document, pleads error or falseness, and the judge decides with regard to the expert supervision and the allegations of the parts. Nevertheless, a suitable legal presumption for the electronic signature validity exists, if the certification service provider is a "accredited" one and the signature used by the signer is officially certificated .

In the case of a simple electronic signature or “not outpost” it only guarantees its admittance as a proof (“test in reason”) that will not reject one directly, by the mere fact of having extended in electronic form .

5. Does the signed document have public document value electronically? ➦

The document by the mere fact of being signed electronically does not become to this in public.

The electronic document will only have class of public, if it fulfils with the requirements required by law, in relation with the arts. 1215 and 1216 of the code of civil law (“Código Civil”)

In this sense, the Law 24/2001, of 27 of December, of fiscal, administrative measurements and of the social order, has introduced a modification in the Law of Notary ("Ley de 28 de mayo de 1862 del Notariado").

The new art. 17 bis contemplates the only made electronic notarial public document of they being written in electronic support with the advanced notarial signature of the notary (and, in his case, of the grantor ones). The notarial authority or intervention of the electronic public document must be subject to the same guarantees and requirements that every public notarial document and producing in consequence the same effects.

6. Which document class can be signed electronically? ➦

In beginning these can be documents of every type. What happens is that we can have specific exceptions.

In the case of an electronic contract, the art. 23 of law 34/2002, (when telling to the hiring by electronic path and to saying the validity and efficacy contracts,) sets that is not possible an application to contracts concerning the rights of family and successions.

Just the same applies to those contracts, juridical business or acts in which the law determines for his validity or for the production of certain legal effects, the public documentary form or that they require by law the intervention of jurisdictional organs, notaries public registers like register of companies, land register etc., which are regulated by the special laws.

In particular, one can use the electronic signature in every kind of documents in the relation to the scope of the citizens with the administration (licence applications, certificates, public bids, tax declarations, etc..) as well as particularly in relations between enterprises and between them and consumers, that is to say in the electronic commercial traffic.

II. Regarding certification service providers ➦

1. Who are certification service providers? ➦

They are public or private companies, physical or legal people who, in terms of free competition, give the service of electronic signature certification, that is to say, they certify that the one that signs an electronic document really uses the keys of that claim to be.

It is more or less an electronic identity card species. In order to be able to certify this previously they have generated the key public and prevailed of the signer and they have identified him.

2. Do all the certification service providers offer me the same guarantees? ➦

No. It is necessary to distinguish between the "credited" and not credited certification service providers. In principle the benefit of these services is free and it is not put under any type of previous authorization, but it exists a voluntary procedure called "accreditation", by which the Administration, previous technical usual evaluations and in case of being these positives, emit one resolution or official document where certifies that this Provider count with the established quality and security rules with regard to their procedures and the products and technology that it uses.

3. How can I be sure which provider is accredited if I do not go to his physical establishment to check it? ➦

All the data of the Providers of Services of Certification established in Spain will appear in the Registry of Providers that is created under the dependency of the Ministry of Justice. It is of public access and it will permanently provide updated information of the main data (e. g. data of identity, direction of homepage, accredited condition, effectiveness of its certificates, etc.)

4. How long does an electronic signature certificate last? ➦

A "recognized certificate, that guarantees a set of information that make them trustworthy, has a limited validity, a maximum period of four years [23] . But before fulfilling this terms we can revoke them and leave them without effect. Also they lose its effectiveness in case of loss or putting out of action, illegal use, death of its holder or in case of cease of its activity by the certification service provider .

5. Can I limit the value of the transactions in which I am going to use my electronic signature as with credit cards? ➦

Yes. It is possible to establish limits in relation to the value of the transactions and to the type of uses in which we anticipate to apply the electronic signature. For it these limits are had to brief clearly in the recognized certificate.

6. Are certification service providers liable in case of fraudulent use of an electronic signature? ➦

In addition to the established general regime of sanctions for the case of breach of its obligations, certification service providers are privately responsible for the damages caused to its user or their contract partners, if they act with negligence [24] .

7. Will my personal data be of free access on the Internet or are they protected? ➦

The personal data of the signatories, as much those that the Certification Service Providers successfully obtains like which they appear in the Registry of Service Providers , are

protected by the Law of Regulation of the Automated Treatment of Personal data of 1992 [25] .

Also, we can use a pseudonym in the certificate of electronic signature, so that our real identity will not be well known by the addressee of the messages.

But in this case the Certification Services Provider is forced to reveal the real identity, when they ask for the judicial organs, and without damage of which it is possible to be established at the scopes of tributary and public security on identification of people.

C. Conclusions ➦

The directive and its implementation in the member-states of the EU guarantees the three essential functions of the electronic signature (to secure the integrity and the authenticity of the document and its non-rejection the origin.) Also in non-member states of the EU, especially in the exceeding-countries, the law concerning electronic signatures are oriented to the community-framework and having similar contents.

This situation of judicial security and clarity and of easy handling is the basis of the current and future success of the e-commerce business. Besides B2B and B2C relationships, the judicial equivalence opens wide chances of a broader application in various other fields, e.g. the further implementation of e-government [26] .

It ´s beyond any question, that the electronic signature is the signature of the future. Of course, the hand-written signature on paper will still play a role, but their importance will decrease more and more. The e-signature will not only take its part in e-commerce and related fields, but will also more and more substitute the hand-written signature in normal day by day business, as the electronic communication will displace the normal communication documented on paper, as can be seen at the astonishing increase of e-mail use in the last years.

D. Bibliography ➦

I. Literature and documents written in English ➦

A List of Certification Authorities maintained by Juan A. Avellan you may see at: http://www.qmw.ac.uk/~tl6345/ca.htm

Ensuring security and trust in electronic com-munication: Towards a European Framework for Digital Signatures and Encryption. COM(97) 503 final. October 1997.

http://www.datenschutz-berlin.de/sonstige/dokument/com97.htm

BSI short information to current topics of IT security:

BSI IT Certificates Information for consumers.

BSI IT Certificates Information for manufacturers.

http://www.bsi.bund.de/english/index/htm

Regulierungsbehörde für Telekommunikation und Post

Digital signatures

http://www.regtp.de/en/index.html

Interdisciplinary Centre for Law and Information Technology (ICRI).

Information concerning digital signature according to countries

http://www.law.kuleuven.ac.be/icri/projects/digisig_lb_eng.htm

John Dickie

Internet and Electronic Commerce Law in the European Union

Hart publishing, Oxford – Portland Oregon, 1999

II. Literature concerning digital signature written in German ➦

Hoffmann, Helmut

Die Entwicklung des Internet-Rechts,

NJW 2001, Heft 14 (Beilage), 5* - 39*

Kuner, Christopher:

Digital Signatures. Law of Commerce in Germany,

http://www.kuner.com

Schmidl, Michael:

Die elektronische Signatur. Funktionsweise, rechtliche Implicationen, Auswirkungen der EG-Richtlinie,

CR 7/20002, 508 -515

Spindler Gerald/ Börner, Fritjof (Herausgeber):

E-Comerce-Recht in Europa und den USA

Springer-Verlag, Heidelberg 2003

Weinknecht; Jürgen:

Digitale Signatur. Gegenwärtige Bedeutung und zukünftige Entwicklung

OJR/2000/10.htm

http://www.ojr.de/index.html?/2000/10.htm

III. Literature concerning digital signature writtenin Spanish ➦

Botana García, Gema Alejandra: (Coordinadora)

Comercio electrónico y protección de los consumidores,

La Ley, Las Rozas (Madrid) 2001

Cremades, Javier/ Gonzales Montes, José Luis:

La nueva Ley de Internet, Comentarios a la Ley 34/2002

La Ley, Madrid 2003

Gómez Segade, José Antonio (Dir.):

Comercio electrónico en Internet,

Marcial Pons, Ediciones Jurídicas y sociales, Madrid 2001

Martínez Nadal, Apol.lónia:

La Ley de Firma Electrónica,

Civitas Ediciones, Madrid 2000

Moreno Navarrete, Miguel Ángel:

Contratos electrónicos,

Marcial Pons, Ediciones Jurídicas y sociales, Madrid 1999

Rosés Sanz, Joacuin:

La Firma Electrónica,

Informática y Derecho 34, p. 225 -243

(Revista iberoamericana de Derecho Informativo), Diputación de Badajoz, 2002

Ribas Alejadro, Javier

Aspectos jurídicos del Comercio Electrónico en Internet

Editorial Aranzadi, Elcano (Navarro) 1999

Vázques Iruzubieta, Carlos:

Comercio Electrónico, Firma Electrónica y servidores. Comentario y anexo legislativo (Ley 34/2002 de 11 de julio)

Editiorial Dijusa, Madrid 2002

E. USEFUL Links

For further information is recommendable to have a look at the following homepages.

http://abanet.org/scitech/ech/

American Bar Association Electronic Commerce Pages

http://www.aece.org

Asociación Española de Comercio Electrónico (Spanish Association Electronic

Commerce)

http://www.commerce.state.ut.us/

Utah Department of Commerce

http://www.legislation.hmso.gov.uk/

“HMSO” Her Majesty’s Stationery Office Online: Legislation in United Kingdom-

http://europa.eu.int

EU homepage, containing links to all the institutions.

(Summaries of European legislation: http://www.europa.eu.int./scadplus)

http://www.mbc.com/ecommerce/international.asp

MCBride Baker and Cole - database to review and search for e-commerce initiatives in any country.

http://www.ojr.de

Online Journal Recht

1: This section has been extracted from European Union’s homepage (www.europa.eu.int/scaadplus/leg/en/lvb/24118.htm) ”Community framework for electronioc signature” ➦

2: See at http://www.commerce.state.ut.us/ ➦

3: See at http://www.meti.go.jp/english/report/data/gesigconte.html ➦

4: COM (97) 157, at III ➦

5: COM (97) 503 ➦

6: Official Journal of the European Communities (OJ L13,19.01.2000, p. 12) ➦

7: The following section has been extracted from the European Commission's homepage (http://www.europa.eu.int/scadplus/leg/en/lvb/24118.htm) ➦

8: Art. 2 .1: "…data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication." ➦

9: Art. 2.2: "... an electronic signature which meets the following requirements: it is unlikely linked to the signatory, … capable of identifying the signatory, … created using means that the signatory can maintain under his sole control,… linked to the data to which is relates in such a manner that any subsequent change of the data is detectable. " ➦

10: See at http://www.oecd.org ➦

11: See at http://www.unicitral.org ➦

12: John Dickie, "Internet and Electronic Commerce Law in the European Union", at page 40 ➦

13: See at article 5 directive ➦

14: See at article 6 directive ➦

15: Regulation in other European states are quite similar. Slovenian Law concerning electronic Signatures, e. g., may you see, as well, at http://e-gov.gov.si/e-uprava/english/pdf/ECAS-Act-_in-English.pdf ➦

16: For further Information see e.g. Spindler/Börner E-Commerce-Recht in Europa und in den USA ➦

17: For further information see http://www.europa.eu.int ; Christopher Kuner, Digital Signatures. Law of commerce in Germany, http://www.kuner.com ; http://www.mbc.com/ecommerce/international.asp ➦

18: See at (http://www.netlaw.de/gesetze/sigg.htm) ➦

19: See at: http://www.legislation.hmso.gov.uk/ ➦

20: For further information in Spanish see: Apol.lónia Martinez, "La Ley de firma electrónica", Madrid 2000; Carlos Vázques Iruzubieta, "Comercio electrónico Firma elctrónica y servidores", Madrid 2002; Francisco Javier Orduña Moreno; "Contratación y Comercio Electrónico"; Davara & Davara, "Factbook Comercio Electrónico", ➦

21: This guide has been extracted and translated from the homepage of the Spanish Ministry of Justice (Ministerio de Justicia Español) : www.mju.es/g_firmaelect.htm ; ➦

22: See also at http://www.regtp.de/en/index.html (about cryptography) ➦

23: Art. 9 RD-Ley 14/1999 ➦

24: Art. 14 RD-Ley 14 /1999 ➦

25: Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal de 1992. This law was on 14-12-1999 derogated by the "Law concerning protection of personal data"(Ley Orgánica 15/1999 de protección de datos de carácter personal"). ➦

26: See about e-government e.g.: Community ´s communication "E-Europe 2005" at http://www.europa/eu.int/scadplus/leg/en/lvb/l24226 ; Program IST Cybervote at http://www.eucybervote.org ➦