Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

The German legal situation after the "Digital Signature Law"

Julia Barcelo, Rosa

Published in:
Droit de l'Informatique et des Télécoms

Publication date:
1998

Document Version
Publisher's PDF, also known as Version of record

Link to publication

Citation for pulished version (HARVARD):
Julia Barcelo, R 1998, 'The German legal situation after the "Digital Signature Law"', *Droit de l'Informatique et des Télécoms*, no. 1, pp. 77-79.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 02. May. 2026

The German Legal Situation after the "Digital Signature Law"

Rosa Julià-Barceló[1]

Introduction

The number of contracts that are entered and performed by electronic means is increasing day by day: It started as a business practice through the use of EDI, and Internet has spread electronic contracting to consumers. This report seeks to provide an overview of legal acceptance of electronic documents and digital signatures according to German law after the approval of the German Digital Signature Act (DSA)[2]. Because Germany is currently, with Italy[3], the only Member State that has a specific regulation on digital signatures and certification authorities (CAs), we consider that this legislation is specially important to the extent it could influence EC legislation on the same issue.

This report begins with a general presentation of the legal requirements concerning contracts and evidence. Following this, a broader description of the new Digital Signature Law will be given. In this context four main issues will be analysed: definitions, licensing, duties and obligations, and liability. In a few cases, we will make comparisons with other laws or proposals, specifically with Community proposals.

Requirements of contract law and evidence law

In general, contract law enjoys the principle of freedom of form, which means that for validity purposes, the contract can be performed in any way (including electronic form). However, the contract needs to be proved in order to be enforced. Documentary evidence (i.e., a written document to which a hand-written signature is affixed) under German law has the benefit of constituting in most cases a reliable means to prove a disputed fact. Documentary evidence benefits from the presumption that the document constitutes evidence of the facts recorded therein unless the other party can prove that the document is not authentic[4]. This rule does not apply to other types of evidence (e.g., proof by witness testimony or proof by inspection); thus, documentary evidence has more evidentiary weight than other types of evidence. Therefore, it is important for the electronic contract to qualify as a document, and thus to be accepted as

---

[1]- Rosa Julià-Barceló is researcher at the Centre de Recherches Informatique et Droit, Namur, Belgium

[2] Federal Act Establishing the General Conditions for Information and Communication Services.

[3]- Schema di Regolamento "Atti, documenti e contrati in forma elettronica", approved by the Italian Council of Ministers 5-8-97.

[4]- BLECHSCHMIDT, R., *The German Basic Electronic Data Interchange Agreement Versus The European Model Agreement: Some Reflections on German Law*, The EDI Law Review, Vol. 3, 1996, P. 107-124

such in court. By using a digital signature and digital certificates to perform the contract, such a requirement might be satisfied.

The DSA was adopted on August 1,1997, with the objective of establishing general conditions under which digital signatures are deemed secure and forgeries of digital signatures or manipulation of signed data can reliably be ascertained. Three month later, following the adoption of the DSA, an Ordinance containing the legal provisions for the implementation of DSA articles 3-15 (eg., grant, withdrawal, revocation of licence, validity periods of signature key certificates, details of the obligations of the CAs) has been adopted[5].

The DSA does not explicitly affect the legal status of electronic documents with digital signature, in other words, the DSA does not establish an equivalence between a hand-written signatures and digital signature as a matter of law governing contracts or as a matter of evidence. However, it can be concluded that by setting out the general conditions for the operation of digital signatures, the law seems to have recognised equivalence between hand-written signatures and digital signatures, when the technical conditions (which ensure authenticity and integrity of the messages) provided in the Act and the Ordinance are fulfilled. In cases of dispute, courts will probably accept electronic documents with a digital signature as documentary evidence. Additionally, the DSA will contribute, through providing a legal framework for the operation of digital signatures and in particular for CAs, towards building mutual trust between parties involved in electronic contracting.

Main Provisions

After having defined digital signatures, certification authorities, certificates and time stamp certificates, the DSA provides detailed provisions on the conditions to be fulfilled by licensed CAs, as well their duties and obligations.

(1) Definitions

(a) For the purposes of the DSA "digital signature" means a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority or the authority according to article 3 of the Act.

(b) For the purposes of the DSA "certification authority" means a natural or legal person who certifies the assignment of public signature keys to natural persons and to this end holds a licence pursuant to article 4 of the Act.

---

[5]- German Digital Signature Ordinance (SigV)

(c) For the purposes of the DSA "certificate" means a digital certificate bearing a digital signature and pertaining to the assignment of a public signature key to a natural person (signature key certificate) or a separate digital certificate containing further information and clearly referring to a specific signature key certificate (attribute certificate).

(d) For the purposes of the DSA "time stamp" means a digital declaration bearing a digital signature and issued by a certification authority confirming that specific digital data were presented to it at a particular point in time.

The DSA has shown a definite choice for a certain type of technology: public key encryption with use of digital certificates issued by CAs. Provided this is used, the two main functions of signatures will be satisfied: establishing the owner of the signature key and integrity of the data.

(2) Licensing CAs

From the various options that were open for the establishment of CAs, the German legislature has chosen a licensing scheme, although this scheme does not appear to be mandatory. According to article 4 of the DSA, a certification authority shall obtain a licence from the competent authority and licences shall be granted upon application. However, because the DSA appears to permit the operation of CAs which are not compliant with the Act, the operation of unlicensed CAs seems to be legal.

The other options could have been the negative licence (any person is free to provide encryption services provided they satisfy certain pre-licensing conditions) or accreditation arrangements. The Commission's recent Communication Towards A European Framework for Digital Signatures and Encryption[6] has stressed the fact that mandatory licensing schemes are a possibility, but that non-licensed but highly recognised private or public organisations might as well be considered as a trusted CA.

[6]- COM (97) 503.

Under the DSA, the applicant will receive a licence provided he possesses the necessary reliability: proof of specialised knowledge (the persons engaged in the operation of the certification authority have the necessary knowledge, experience and skill) and guaranteed compliance with legal provisions applicable to the operation of such an authority. The Ordinance contains detailed description of the application for licence procedure including costs.

(3) Duties and Obligations

The DSA provides, inter alia, for the following obligations:

Article 5 states that the CA will have to *reliably establish the identity* of persons applying for a certificate as well as information concerning their professional status.

The CA must *issue certificates* and *take measures* to prevent undetected forgery or manipulation of data as well as to ensure confidentiality of private signature keys.

The CA will *notify* the applicants of the measures necessary to support secure digital signatures and their reliable verification.

Article 8 contains an obligation concerning the invalidation of certificates where the owner of a signature key requests it, when the certificate was obtained through certain false statements. It should be noted that the DSA does not address the issue of whether the CA should be required to provide a full 24-hour service for invalidating certificates.

(4) Liability

Unlike other laws or proposals, the DSA does not address liability issues. Legal comments argue that regulation has been postponed until more consensus has been achieved about which kind of rules should be established. Therefore, at the moment, the general liability rules shall apply. In case of tort liability, this means that a with-fault liability regime will be applicable. The licensed CA, as described above, has the statutory obligation to issue certificates and to establish and maintain a database of revoked certificates. Thus, the CA should assume responsibility for the accuracy, the updating and completeness of its certificates and database *vis a vis* its own subscribers.

The criteria of duty of care would seem to be a good one. However, because of the technical issues surrounding the certification process, it will be very difficult for consumers to prove the lack of care of the CA in the issuance of a certificate. Consequently, we suggest that the *onus probandi* should be reversed. This means that it should be sufficient for the damaged subscriber and third party to assert that the CA did not exercise sufficient care in the carrying

out of his obligations and it will be up to the CA to evidence the contrary by proving the satisfaction of the requirements set out in the DSA and Ordinance.

Conclusions

According to German law, the use of electronic means to enter contracts does not raise special problems but some doubts: First, will the parties involved in such electronic contracts trust the system and feel confident about the security? Second, as a matter of evidence, will the electronic document be valued as documentary evidence?

The implementation of the DSA will provide a positive answer to the above questions. First, the contracting parties in an electronic transaction will be confident that by using a digital signature and a digital certificate issued by a licensed CA, they have a much more trustworthy system than ever before. Second, the document issued using these techniques will have the same evidentiary value as documentary evidence. However, the DSA, by imposing such strict conditions for becoming a CA, may discourage business from engaging in CA activities. In addition, the DSA suffers from its failure to address, from the point of view of consumer protection, the liability questions identified above.

Overall, the DSA is a good starting point towards achieving security in electronic communications.