



Internationaler Archivkongress 2004  
23.-29. August - Wien - Österreich

**Archive, Gedächtnis und Wissen**



# Problems of Authenticity in an Electronic Environment

Josef Zwicker

Udo Schaefer

Laura Millar

---

## Problems of Authenticity in an Electronic Environment: Authenticity - Electronic Signatures or Trusted Custodian?

Udo Schäfer

---

### 1. Introduction

*As a society, we want our leaders and the people who act in our name to be accountable for their actions, and records play a role in rendering that account. So it is in our interest to establish standards for reliable and authentic records, and archivists have a role to play in achieving that objective.*<sup>1</sup>

Heather MacNeil, School of Library, Archival and Information Studies of the University of British Columbia, uses this sentence to explain why archivists have to deal with the following question: How can the authenticity of electronic records be ensured? An authentic record is a record that can be proven

1. to be what it purports to be and
2. to be free from falsification and unauthorized alteration.<sup>2</sup>

One measure to prove the authenticity of electronic records is the use of digital signatures.

Digital signatures are based on a public key cryptography, which use algorithmic functions to create a compressed form of the document called the hash result and to generate two different but mathematically related keys called the public and the private key. The digital signature is created by encoding the hash result with the private key. Attached to the document the digital signature will be stored or transmitted with the document. The verification will confirm the authenticity of the document if

1. the digital signature can be decoded with the public key,
2. a new hash result created of the stored or transmitted document is identical with the decoded hash result,
3. a certificate issued by a certification service provider proves that the public key belongs to the person who is named as the author of the document,
4. the digital signature has been generated within the period of validity of the certificate and
5. the algorithmic functions have not lost their applicability as a result of technological advance.

The notion of the digital signature is covered by the broader conception of the electronic signature. The common purpose of the different kinds of electronic signatures is to provide functional equivalents to handwritten signatures and to other authentication measures in a paper based environment.<sup>3</sup>

### 2. The Law on Electronic Signatures

#### 2.1 The International Law

In 1966 and 1967, the United Nations Commission on International Trade Law (UNCITRAL) has been established by the United Nations to enhance the harmonizing of the commercial law. The commission has published the UNCITRAL Model Law on Electronic Commerce<sup>4</sup> in 1996 and the UNCITRAL Model

---

<sup>1</sup> Heather MacNeil, Trusting Records in a Postmodern World. In: *Archivaria*, No. 51, Spring 2001, p. 46.

<sup>2</sup> Authenticity Task Force Report, p. 2. In: *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPares Project*, September 2002 (URL: <http://www.interpares.org>. Retrieval: 2003-08-05). – Heather MacNeil, Providing Grounds for Trust: Developing Conceptual Requirements for the Long-Term Preservation of Authentic Electronic Records. In: *Archivaria*, No. 50, Fall 2000, p. 53. – Idem, Providing Grounds for Trust II: The Findings of the Authenticity Task Force of InterPARES. In: *Archivaria*, No. 54, Fall 2002, p. 26.

<sup>3</sup> Cf. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, New York 2002 (URL: <http://www.uncitral.org>. Retrieval: 2002-07-10), pp. 19–31.

<sup>4</sup> UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 (URL: <http://www.uncitral.org>. Retrieval: 2003-09-16).

Law on Electronic Signatures<sup>5</sup> in 2001. A broad conception of the signature is used by the UNCITRAL Model Law on Electronic Commerce in article 7 para. 1:

*Where the law requires a signature of a person, that requirement is met in relation to a data message if:*  
(a) *a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and*  
(b) *that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.*

This broad notion has been adopted by the UNCITRAL Model Law on Electronic Signatures. In article 6 para. 3, the Model Law describes the requirements for a reliable electronic signature:

*An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:*  
(a) *The signature creation data are, within in the context in which they are used, linked to the signatory and to no other person;*  
(b) *The signature creation data were, at the time of signing, under the control of the signatory and of no other person;*  
(c) *Any alteration to the electronic signature, made after the time of signing, is detectable; and*  
(d) *Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.*

The purpose of article 6 is to ensure that the electronic signature is equivalent to the handwritten signature.

## **2.2 The European Law**

The Council of Europe and the European Union have to be distinguished. These supranational organisations are independent from one another. Whereas the recommendations of the Committee of Ministers of the Council of Europe to member states have to be considered as soft law, the member states of the European Union are obliged to transfer the directives of the European Parliament and of the Council into national law.

### **2.2.1 The Council of Europe**

In 2003, the Committee of Ministers of the Council of Europe has adopted the Recommendation Rec(2003)15 on archiving of electronic documents in the legal sector<sup>6</sup>. The recommendation provides in principle 7.2 a rule concerning the probative force of electronic documents transferred to archiving services:

*An archived electronic document should be considered reliable and valid, in the absence of proof of the contrary, regardless of the possibility of continuous verification of its initial electronic signature, provided that it has been transmitted to and preserved by archiving services in accordance with the security requirements as specified in Principle 4.*

---

<sup>5</sup> UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 (Note 3).

<sup>6</sup> Recommendation Rec(2003)15 of the Committee of Ministers of the Council of Europe to member states adopted on 9 September 2003 on archiving of electronic documents in the legal sector (URL: <http://www.coe.int>. Retrieval: 2004-07-16).

After the transfer to archiving services electronic documents should be considered authentic if they have been transferred and preserved in accordance with special security requirements, even though the electronic signatures could no longer be verified.<sup>7</sup>

### 2.2.2 The European Union

The member states of the European Union had to transfer 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<sup>8</sup> and the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures<sup>9</sup> into the national law. The Directive on electronic signatures differentiates between

- 1) the electronic signature,
- 2) the advanced electronic signature, and
- 3) the advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device.

Article 2 of the directive defines the electronic signature and the advanced electronic signature as follows:

Electronic signature *means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.*

Advanced electronic signature *means an electronic signature which meets the following requirements:*

- (a) *it is uniquely linked to the signatory;*
- (b) *it is capable of identifying the signatory;*
- (c) *it is created using means that the signatory can maintain under his sole control; and*
- (d) *it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.*

The third category of electronic signatures, the advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device, shall be called with reference to the German law qualified electronic signature. Merely the digital signature, which is based on a public key cryptography, meets currently the conception of the qualified electronic signature.

The Directive on electronic signatures authorizes the member states to introduce a voluntary accreditation of certification service provider and to define additional requirements for the use of electronic signatures in the public sector. With regard to the private sector, the Directive on electronic commerce requires in article 9 the legal equalization of contracts concluded by electronic means with paper based charters, while the Directive on electronic signatures demands in article 5 that the qualified electronic signature should be supplied with the same probative force as the handwritten signature by the private and the public law.

### 2.3 The Limitations of Electronic Signatures

*Even if one bit in the message has been altered after the message has been digitally signed, the message digest created by the relying party will be different from the message digest created by the signatory.*<sup>10</sup>

The migration of electronic records, which is an essential element of the preservation strategy, makes it impossible to verify the digital signatures. Therefore the following question has to be answered: How shall the national legislation deal with the fact that the use of digital signatures ensures the authenticity of electronic records only for a short period of time? Neither the UNCITRAL Model Laws nor the

---

<sup>7</sup> Recommendation Rec(2003)15 of the Committee of Ministers of the Council of Europe to member states adopted on 9 September 2003 on archiving of electronic documents in the legal sector. Explanatory Memorandum, No. 57 (URL: <http://www.coe.int>. Retrieval: 2004-07-16).

<sup>8</sup> Official Journal of the European Communities 2000, L 178, pp. 1–16.

<sup>9</sup> Official Journal of the European Communities 2000, L 13, pp. 12–20.

<sup>10</sup> UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 (Note 3), p. 31.

---

Directives of the European Union offer a solution for this problem. However, the Recommendation of the Council of Europe solves the problem by replacing the electronic signature by a trusted custodian.

### 3. Conclusion

In 2003, the German Federal Ministry of Justice has produced a first draft to amend the German Civil Procedure Act in order to transfer article 9 of the Directive of the European Union on electronic commerce and article 5 of the Directive of the European Union on electronic signatures into the German law. The new article 371 a shall supply private and public electronic documents provided with a qualified electronic signature with the same probative force as paper based private and public charters. The State Archives of the German Federal State of Hamburg have submitted a statement to the first draft of the amendment. Among others the statement proposes with regard to public electronic documents to add the following provision to the new article 371 a:

*The rules concerning the probative force of public charters shall apply to public electronic documents which were provided with a qualified electronic signature until they have been converted into a different technical format and transmitted to public archives if*

- 1) *a verification in accordance with the Signature Act has been conducted immediately previous to the conversion and the transmission,*
- 2) *the results of the verification and the documentation of the transmission have been attested by an attestation and*
- 3) *the public archives have chosen procedures for the transmission and the preservation which have to be considered as suitable to protect electronic documents against falsification.*

*If the requirements mentioned in Sentence 1 have been met Article 437 is applicable.*

Paper based public charters have been provided with the presumption of authenticity by article 437 of the German Civil Procedure Act.

The German Federal Ministry of Justice has published a second draft<sup>11</sup> on July 28, 2004. The suggested provisions have not been added to the new article 371 a. The refusal was not unexpected, because governments are seldom aware of the role of public archives in juridical and administrative matters. Therefore, the insertion of the following sentences in the explanatory memorandum was a great surprise:

*If an electronic document already transferred to the responsible public archives is needed as a piece of evidence in legal proceedings the requirements for the preservation prescribed by the archives acts are decisive. If these requirements have been met the electronic documents are equally supplied with the probative force granted by article 371 a.*

The German public archives will have made an important step towards the recognition as trusted custodians in an electronic environment if the explanatory memorandum of the bill still contains these sentences.

---

<sup>11</sup> Entwurf eines Gesetzes über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG). <http://www.bmj.bund.de>. Retrieval: 2004-07-30.