ARTICLE:

ELECTRONICALLY SIGNED DOCUMENTS: LEGAL REQUIREMENTS AND MEASURES FOR THEIR LONG-TERM CONSERVATION[1]

WRITTEN BY:
STEFANIE FISCHER-DIESKAU
AND DANIEL WILKE

Electronic signatures are an important technology to provide for the integrity and authenticity of electronic documents.[2] In contrast to paper based documents however, the security value of electronically signed documents can decrease in the course of time. This is particularly due to technical developments in respect of the security of cryptographic algorithms. Furthermore, the availability of the relevant information to verify an electronic signature cannot be guaranteed. Finally, the rapid development of the software market endangers the readability of the documents. The necessary technical and organisational solutions to these problems need to comply with legal requirements. This article examines these requirements, and considers the consequences for the technical design and for the development of the law.

Relevance of archiving documents

Documents are generally generated and archived for several reasons. They serve not only as an aid to the memory for past events, but they have a great importance for the settlement of disputes and proving assertions in litigation. German law therefore provides for several obligations to keep records for different retention periods. Pursuant to the German Commercial Code and Fiscal Code, for example, traders are required to keep books and records for up to ten years, to comply with accounting rules and legal provisions. For instance, medical documents, which physicians generate in order to comply with the duty to document an event, have generally to be kept for ten years; however much longer periods can be necessary, subject to the specific type of medical treatment. Hence, some documents need to be archived for 30 years or more in a secure and conclusive way. This means the integrity and authenticity, as well as the readability of the document, has to be maintained for the relevant retention period. These requirements apply to all documents independent from the form in which they are generated and archived.

Signature-specific issues of electronic archiving

For documentation in a paper-based form, complying with requirements of retention only makes demands on the quality of the paper and the storage environment. In respect of electronic documents, however, further measures have to be taken in order not only to prove the integrity and authenticity of the document at the time of its generation, but also throughout its entire relevant retention period. Although electronic

[1] *The article refers to results developed in the projects ArchiSig – Conclusive and secure long-term archiving of digitally signed documents - and TransiDoc – Legally secure transformations of signed documents, both funded by the German Federal Ministry of Economics and Technology. For further information see www.archisig.de and www.transidoc.de.*

[2] *The term elelctronic signature is used in this article, rather than digital signature, following the wording of the European Union Directive on electronic signatures and the German Law.*

The European directive on electronic signatures does not contain provisions regarding the long-term preservation of electronically signed documents.

signatures are a significant technology to secure the integrity and authenticity of electronic documents, further measures have to be taken to enable the conclusive storage of the documents for ten years or more. This is the result of technical developments: hash and public key algorithms can lose their security suitability over the course of time, which can endanger the integrity of electronically signed documents after a long period of time. Furthermore, the permanent availability of the directories needed for the verification of the signature cannot be guaranteed. Therefore, the value of evidence of electronic signatures needs to be preserved actively before the deterioration of the security of the cryptographic algorithms employed, and the loss of the verification data.

The European directive on electronic signatures does not contain provisions regarding the long-term preservation of electronically signed documents.[3] It is suggested that the directive should have provided for the long-term preservation of documents in electronic format. Pursuant to Annex II (i) of the directive, the certification-service-providers issuing qualified certificates are only obliged to record all relevant information concerning a qualified certificate for an appropriate period of time in order to provide evidence of certification for the purposes of legal proceedings. The term “appropriate period” is, however, not further specified. The German legislator has decided to pass national legislation to regulate by law measures to prevent the loss of evidential probity.

German Law provides a procedure to re-sign the signature to deal with the possible loss of security of the hash and public key algorithms used to affix a digital signature to an electronic document. The specific requirements are stated in section 6 of the Signatures Act and section 17 of the Signatures Ordinance.[4] The relevant text reads, in an unofficial translation

> “the data shall be furnished with a new qualified electronic signature prior to the time at which the suitability of the algorithms and related parameters ends. This signature shall be furnished with suitable new algorithms or related parameters, include earlier signatures and bear a qualified time stamp.”

The new electronic signature is not a declaration of intent, but a means of providing further security for the original signed document. Therefore, it is irrelevant who adds the new signature; it can be any natural person who is the owner of a qualified certificate in accordance to article 2(10) of the directive. Adequate hash and public key algorithms have to be used when a document is signed with a new electronic signature and the action should take place before the original cryptographic algorithms lose their ability to remain secure. Being the competent authority for accrediting and supervising all notified certification service providers, the German Federal Network Agency has the duty to publish in the Federal Bulletin at least once a year an overview of the suitable algorithms, as well as the duration of the suitability of the algorithms.[5] The latter period should last at least six years after the time of assessment and publication.

Section 17 of the Signatures Ordinance states that the data shall be re-signed. These can be the original data which were initially signed, including the content of the document itself, or the hash-data as representative of the content. The recourse to the content is useless if only the security suitability of the

[3] *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.*

[4] *Law Governing Framework Conditions for Electronic Signatures (Signatures Law - SigG) of 16 May 2001 (Federal Law Gazette I, p. 876), last amended by Art. 1 of the First Act Amending the Signature Law (First Signatur Amendment Act -1. SigÄndG) of 4 January 2005 (Federal Law Gazette I, p. 2). Ordinance on Electronic Signatures (Signatures Ordinance) of 16 November 2001 (Federal Law Gazette I, p. 3074), last amended by Article 2 of the First Act Amending the Signatures Act of 4 January 2005.*

[5] *See Annex 1, part 2 of the Signatures Ordinance.*

Further measures have to be taken to ensure the verification of the electronic signature and thereby the authenticity of the electronically signed document.

public key algorithms is endangered. In this case the content is still represented by the original hash-data. Therefore is it sufficient to renew the signature affixed to the document.[6] It is only where the hash procedures become insecure, that the new electronic signature needs also to include the content of the document. In all other cases, the renewal of the signature must only include all existing signatures. The renewed electronic signature can be carried out automatically by using only a qualified time stamp, in case the time stamp contains a qualified electronic signature according to the Signatures Act. A second qualified signature would not bring a further added value.[7] The renewed electronic signature can refer to several documents.

Further measures have to be taken to ensure the verification of the electronic signature and thereby the authenticity of the electronically signed document. Although the German Signature Law provides legal obligations for certificate service providers to retain certificates in their directories for at least five years from the end of the year in which the validity of the certificate terminates, and for accredited certification service providers the period amounts to 30 years, longer archiving periods may occur. Hence, all verification data necessary to prove the existence and validity of the certificate related to the signature have to be archived as well.

Format-specific issues of electronic archiving

Apart from the difficulties related to the loss of the security of the algorithms, the long-term preservation of signed documents makes it necessary to solve the problems that arise from the need to transform the documents from one technical format into another.

In the life-cycle of a document that is to be archived for a long period, multiple transformations in different forms are almost inevitable. First, the original document often needs to be migrated into a suitable archiving format. Hence, where a paper document is to be included into an electronic archiving system, it has to be scanned and thus to be transformed into an electronic document. A similar procedure is needed if the original has been generated in electronic form from the start. For electronic documents, it is necessary to convert the document into one of the software formats that have been chosen for the archiving system. Second, given the rapid development of the software market, it will be essential to transform the electronically stored documents into new data formats before the old ones become obsolete. Otherwise it would be impossible to guarantee the permanent readability of the archived materials. Finally, it is by no means sure that in the near future everyone who wishes to use a document in legal relations will have adopted an entirely electronic workflow. Therefore, it will still be necessary to print electronic documents and transform them into paper documents in order to make them available to the reader.[8]

The changed meaning of certified copies in the digital world

Under section 435 of the German Code of Civil Procedure, a high probative value is accorded to copies of a public paper document if they are certified by a public authority or a notary. Since the enactment of the Third Act Modifying Administrative Procedures[9] and the Judiciary Communications Act,[10] German law also provides for the certification of electronic images of paper documents, of electronic documents which have a software format other than the electronic original, and of printouts of electronic documents. However,

[6] *Roßnagel/Fischer-Dieskau/Pordesch/Brandner, Erneuerung elektronischer Signaturen, CR 2003, 301 ff. This interpretation is disputed, Skrobotz, in: Manssen, Telekommunikations- und Multimediarecht, volume 2, november 2004, § 17 SigV no. 26 sees it as not compatible with the rules of interpretation.*

[7] *Roßnagel/Fischer-Dieskau/Pordesch/Brandner, Erneuerung elektronischer Signaturen, CR 2003, 301 ff.*

[8] *Roßnagel, Das elektronische Verwaltungsverfahren – Das Dritte Verwaltungsverfahrensänderungsgesetz, NJW 2003, 469, 474.*

[9] *Federal Law Gazette (BGBl.) 2002 Part I, p. 3322.*

[10] *Federal Law Gazette (BGBl.) 2005 Part I, p. 837.*

Despite its obvious advantages however, the transformation of signed documents always involves the risk of falsification.

these different kinds of certifications also have different purposes. Certifying a paper copy serves as a means to multiply the original document so that the bearer can present it to several other persons or institutions without having to relinquish the original. After copying it, the owner will preserve this source document in the archive.

By contrast, scanning a document or converting it into another format serves a completely different purpose. Once an archivist has scanned a paper document and saved the electronic document on a data medium, the latter can be copied and sent away as often as necessary. Nevertheless, the archiving body does not have to dispose of its own electronic copy. The same applies where an electronic document is transformed into another format. As in these cases, an electronic copy of the original document always remains with the archiving body, it is usually in its interest to destroy the paper or electronic source document in order to save storage space. Hence, in the case of format changing copies, the certification aims at making the preservation of the original completely expendable.

Technical risks

Despite its obvious advantages however, the transformation of signed documents always involves the risk of falsification. Moreover, during the process of transformation, the technical security measures lose their functional capability. Thus, the handwritten signature in a paper document loses its probative value when it is scanned. In this case, it is impossible to tell whether the signature was really part of the original document or if it has been electronically copied into the target document. Similarly, once an electronic signature has been transformed into another software format, the electronic signature cannot be verified in the target document that is generated in the transformation process, but exclusively in the source document.[11] Furthermore, data and metadata might get lost during the conversion because of technical failures. There is also a certain danger that the target documents might be manipulated after the transformation.

The risks set out above constitute serious difficulties for the use of transformed target documents in legal and commercial relations. Hence, there is a need for suitable technical transformation systems that will allow the preservation of probative value in the target document that is comparable with the probative value of the source document. In the interest of cost-effective document management, it is desirable to create an automated transformation process and to design it in a way which makes the preservation of the source document unnecessary. Furthermore, it is important to introduce a legal framework to legally secure transformation systems.

Requirements to legally secure transformation of signed documents

The target document can only be an equivalent replacement for the source document if it attests that the latter had certain legally relevant properties, and that the target document corresponds with it. Legally relevant properties are, for instance, the form of the document as well as information about the author's handwritten or electronic signature. Therefore, it is recommended that the certifying institution should attach an attestation clause to the target document which attests that the source document has these properties, and that the two documents correspond with each other. For the sake of legal certainty, the law should define how integrity and authenticity of the source document are verified by the certifying institution and which verification data the attestation

[11] *The term source document refers to the document that is introduced into the transformation process. It is not necessarily the original as it may have been generated in a former transformation process itself.*

[12] *German Law contains such provisions under section 33 of the Administrative Procedures Act.*

clause must contain.[12]

Furthermore, it is of vital importance to develop technical procedures that allow for a secure transformation. To protect the system against mistakes that might be caused by human intervention, a fully automated process would be preferable. In this case, the administrator of the transformation system could carry out subsequent random tests by comparing several source and target documents.[13] In order to avoid manipulation of the process, it must be made sure that only authorised persons have access to the transformation system. If clear rules on these issues are laid down and obeyed, secure transformation systems could be established that are run by public authorities, notaries public or private entities. A public body could certify the systems so that target documents generated by them would receive a higher probative value.

Electronic documents and the law of evidence

Electronic documents are, independent from the existence of an electronic signature, admissible as evidence in court. Where the genuineness of a document is questioned, the party invoking its originality is responsible to proving it.[14] In practice, the genuineness is made evident by means of a technical expert witness. A judge is, in general, free to appreciate whether or not to consider the document as genuine. However, electronically signed documents based on a qualified certificate enjoy a higher degree of evidence: under German Procedural Law these documents are presumed genuine unless there are justified doubts that the signed declaration originates from the holder of the private cryprographic key.[15] The application of this provision depends on a timely re-signing of the document that conforms to the requirements laid down in section 17 of the German Signatures Ordinance, and the availability of all necessary verification data to verify the signature. If these measures have not been taken, the document is not worthless, but the proof of genuineness may be difficult where the authenticity of the document is questioned.

Regarding transformed documents in other formats, some legal systems have so far not yet taken into account the practical need for replacing original documents. Under German procedural law, for instance, a private paper document can only deploy its full probative force, if the original is presented to the judge.[16] In this case, the document provides full proof for the declarations it contains, a rule which is binding for the judge.[17] If the party presents only a copy of the document, the judge can consider the evidence freely without being bound to regard the declarations set down in the document as true facts. Public documents, by contrast, can also be presented in the form of certified copies.[18] However, even if the transformation system provides for maximum security, a transformed target document can only be regarded as a certified copy of the original. Hence, the law in force impedes the use of transformed documents in evidence.

This situation gives rise to the question of whether the different legal treatment of private and public documents is still adequate in the course of the change to electronic document management systems. Given the high level of security which is provided by electronic signatures, the integrity and authenticity of an electronic source document can be established with far greater reliability than in the case of a paper document bearing a handwritten signature. Where, moreover, a trustworthy institution like an administrative authority, a notary or a certified private organisation verifies these points as well as confirming the source and the target document, it seems appropriate to attribute a probative value to the target document which is comparable to that of the source document. If these requirements are met, it should not matter whether the document in question originates from a private person or a public authority.

Dr. Stefanie Fischer-Dieskau and Daniel Wilke, LL.M. are solicitors and members of the Project Group Constitution Compatible Technology Development at the University of Kassel headed by Prof. Dr. Alexander Roßnagel where they work on the research projects "ArchiSig - Conclusive and secure long-term archiving of digitally signed documents" (www.archisig.de) and "TransiDoc – Legally secure transformations of signed documents" (www.transidoc.de).

s.fischer-dieskau@uni-kassel.de
d.wilke@uni-kassel.de
http://www.uni-kassel.de/fb7/oeff_recht/

[13] *Human control during the transformation process might be necessary where an encrypted document is introduced into the transformation system, decrypted to allow for the format conversion and re-encrypted right afterwards.*

[14] *For paper documents see Federal High Court of Justice, Neue Juristische Wochenschrift 2000, p. 1180 et seq.*

[15] *Section 371a of the Code of Civil Procedure.*

[16] *Section 420 of the Code of Civil Procedure.*

[17] *Section 416 of the Code of Civil Procedure.*

[18] *Section 435 of the Code of Civil Procedure.*