Digital signatures and electronic records

Filip Boudrez
Expertisecentrum DAVID vzw
Antwerpen, 2005

0. TABLE OF CONTENTS

1. INTRODUCTION

Electronic records have the advantage that they are reusable. One can very quickly adapt a record or compile a new record on the basis of an existing one. This digital advantage is at the same time a vulnerability because adaptations or changes are not always observable. Because of this, the reliability of electronic records might be questioned.

Finding methods for guaranteeing the reliability of digital documents in general, or electronic records in particular, is the subject of research in various professional fields. At present, one of the most widely suggested solutions is digital signing electronic records. More specifically, the use of asymmetric cryptography and the digital signature is advanced as a proof of authenticity and integrity for electronic records. This technique might also be usable to ensure the reliability of electronic records[1].

The use of digital signatures, and especially archiving digitally signed documents, has been keeping archival science occupied for some time now. Archivists are not only being confronted with the preservation of digitally signed documents, but more and more people are also suggesting the use of the technology of the advanced digital signature to ensure the authenticity and integrity of all electronic records in custody of the archivist. This would mean that the archivist or the creator would have to sign all electronic records kept in the archives. The integrity of electronic records could be checked by a verification of the signature of the archivist or the creator. The archiving strategy called the Victorian Electronic Records Strategy (VERS) is probably the best-known example of this[2].

It quickly became clear, however, that archiving digitally signed documents raises a number of questions and difficulties. This paper wants to give an overview of the archival issues that relate to

---

1 D. Pinkas, *Long-term preservation of signed documents,* at: *e-Archiving for posterity*, Leuven, 26 June 2003; S. Hackel, T*he ArchiSafe Project - legally secure and scalable long-term record keeping complying with the requirements of the German electronic signature law*, at: *DLM Forum 2005*, Budapest, 6 October 2005.

2 http://vers3.imagineering.net.au

digitally signed documents[3]. First, by way of introduction, the advanced digital signature is presented briefly. In the second part, a number of problems are discussed that present themselves when a digital signature is used as a proof of authenticity and integrity for digital documents in general. In particular, it is also being investigated whether it makes any sense for the archivist to digitally sign all electronic records under his or her management. Problems relating to the (medium) long-term archiving of digitally signed documents are dealt with in the third part. After an overview of the sticking points for long-term validation (4.1) a number of possible solutions are discussed (4.2).

In this contribution, the concepts *authenticity* and *integrity* are used as they have been defined by the InterPARES project[4]. Authenticity and integrity are essential characteristics of a reliable or trustworthy record. A record is authentic if it is what it purports to be and if it was created or sent by the person who claims to have sent it. Integrity means that the record is complete and unaltered. This does not mean that records may not experience any changes, but it does mean that records must be protected against tampering or corruption and that it's clearly defined which changes or annotations may occur after the creation or capture as record.

Thus, integrity does not mean that records must be identically the same as they were when created or received. The integrity of a record means that its function and finality has not been changed. Essential characteristics or components of a record may not be modified. Incidental characteristics or components on the other hand may be modified or may even be lost. This view is based on the premise that the original electronic records are doomed to disappear as a consequence of technological obsolescence and that changes and/or loss are therefore unavoidable. What we can preserve is the possibility of reconstruction, and preserve the records “as close to the original as possible.”

2. THE ADVANCED DIGITAL SIGNATURE

The technology of the advanced digital signature makes use of an asymmetric key pair: the private key and the public key. The private key serves to generate a digital signature and/or to decrypt encrypted information. The private key must remain secret, whereas the public key is published. The public key is used to check a digital signature and/or to send confidential information in an encrypted form. The private and public keys cannot be derived from each other. This key pair is, as a rule, issued by a certification authority that verifies and registers the identity of the signer[5], but it can also be created by the user himself[6].

Signing a digital document with an advanced digital signature is a two steps process. The computer file that contains the document is first hashed. This is the conversion of a computer file into a unique code on the basis of an algorithm. This produces a hash value that, in the second step, is then encrypted with the private key of the sender. The result of that operation is the digital signature which is a separate digital object. The sender sends the digital document together with the digital signature to the

---

3 With thanks to Hannelore Dekeyser and Inge Schoups for their suggestions and comments.

4 INTERPARES AUTHENTICITY TASK FORCE, *Requirements for assessing and maintaining the authenticity of electronic records*, in: InterPARES, *The long-term preservation of authentic electronic records: findings of the InterPARES project*, 2002, p. 2-3.

5 The operation of PKI and digital signatures is described in detail in: P. VAN EECKE, *Naar een juridische status voor de elektronische handtekening: een rol voor de handtekening in de informatiemaatschappij?*, doct. diss. law degree, Leuven, 2004, p. 328 ff.; S. VAN DEN EYNDE and J. DUMORTIER, *De rol van de digitale handtekening bij de archivering van elektronische documenten*, Leuven, z.d. (http://www.Antwerp.be/david/website/teksten/DAVIDbijdragen/Digital_signature.pdf); S. HUYDECOPER and S. VAN DER HOF, *De handtekening: van geschreven naar elektronisch*, in: *Archiefbeheer in de praktijk*, 42, 1565; http://www.digitalehandtekening.be.

6 For example: Pretty Good Privacy, OpenPGP, GnuPG.

receiver. The digital document itself can also be encrypted with the public key of the receiver, but this is not necessary. The receiver confirms the validity of the document by decrypting the digital signature with the public key of the sender. After decryption, the hash value of the digital document appears. Then, after a recalculation of the document's hash value, the receiver can compare the hash value that has just been calculated with the hash value that was sent with the document.

An advanced digital signature has in theory three functions:

- authentication: the digital signature was created with the private key of the sender
- integrity: proof that the document has not been changed after it was signed
- 'non-repudiation': the signer cannot deny that he has sent or signed the document.

By itself, a digital signature says nothing about the true identity of the sender, since it essentially relates only to a unique code. For the verification of a digital signature, the link between the sender and his public key must be evident from a digital certificate. Just like the key pair, the digital certificate can be created by the sender himself or by an (authorised) intermediary like a certification authority. A digital certificate from a certification authority provides a higher degree of reliability because digital certificates are only as reliable as the person or the agency that supplies them. When the advanced digital signature is realised with a qualified certificate, the signature is called a qualified digital signature. With each key pair, certification authorities supply a digital certificate that contains the public key and information about the identity of the owner of the key, the validity period, the signature algorithm, the serial number of the certificate and the name of the certification authority. Digital certificates have a limited validity period, but they can also be revoked before the expiration of this period. The owner of the key can request the revocation of the certificate if the private key is lost or stolen. To verify the reliability of the certificates, digital certificates themselves are signed with the private key of the certification authority. The certificates of the certification authority are verified with the public key of the certification authority. This requires a root certificate that links a certification authority with a key pair. Thus, for the verification of a digital signature, an entire validation chain is necessary. It is not sufficient just to archive the document and the digital signature if one wants to validate a digital document with a digital signature in the future.

3. DIGITAL SIGNATURES AS PROOF OF AUTHENTICITY AND INTEGRITY

Digital signatures are commonly presented as a proof of the authenticity and integrity of digital objects. But electronic records are more than just digital objects or documents[7]. In this chapter will be examined whether digital signatures can demonstrate the authenticity and integrity of electronic records and if so, whether they are sufficient as the only proof of authenticity and integrity.

3.1 Digital signatures are seals

For several types of documents, the Belgian legislator gives a qualified digital signature the same judicial value as a hand-written signature. In archival literature attention is drawn to a practical difference in the way that both signatures are linked to a person. In the case of a digital signature, everyone who possesses the private key can sign a document. A digital signature is therefore also

[7] For the distinction between a computer file, a digital document and an electronic record, see: F. BOUDREZ, *A. Inleiding. 2. Digitaal archiefdocument*, in: F. BOUDREZ and H. DEKEYSER, *Digitaal archiefbeheer in de praktijk. Een handboek,* Antwerp-Leuven, 2004.

often compared with a digital seal[8]. The digital signature proves that someone who was in the possession of the private key signed the document. The digital signature does not prove automatically that person X signed the document, but it does prove that the document was signed by someone who had access to the private key of person X[9].

The guarantee that the document actually was signed by the person whose private key was used, depends on the security of the private key. In the PKI model, the end-users are responsible for the management of their private keys. Since private keys are preserved digitally and current computer operating systems are not always 100% safe, special precautions are necessary for the safe storage of private keys. Just like seals, digital signatures are separate objects that can be stolen or copied[10]. The value of the digital signature depends therefore on the procedure in which the digital signature is used, the association between private key and owner, and on the safe storage of the private key[11].

The legislator is himself conscious of this problem. Thus the legislation also includes a liability regulation in case of loss or theft. The owner of the key is responsible for each use of his private key until the time that he has the associated digital certificate revoked.

3.2 Authentication isn't depending on the identity of documents

The validation of digital documents by means of a digital signature corresponds with authentication or the demonstration of authenticity. A digital signature checks the validity of a document on the basis of the bitstreams (physical form) and in doing so it does not take any account whatever of the identity of the document (intellectual form).

The authenticity of a document is related to its integrity and identity. In function of the identity of a digital document, its authenticity is investigated. In other words, the authenticity of a digital document depends on how a document is presented or identified. A forged document that is presented as such, is authentic, whereas a forged document that is presented as "real" is not authentic.

The authenticity of a document can only be shown if the identity of the document is established. In the identity, the unique characteristics and the distinguishing characteristics of a digital document are registered so the difference with other records is clear. The extent of authenticity cannot be researched without the essential characteristics of a record being registered and identified in a meaningful way. The identity of a document cannot be established with a digital signature. Also in the PKI model, the establishment of identity is not enforced in any way whatever.

---

8 INTERPARES, *The InterPARES Glossary*, 2001, p. 3; J. CURRALL, *Digital Signatures: not a solution, but simply a link in the process chain*, Glasgow, 2002, p.3 (http://eprints.lib.gla.ac.uk/documents/disk0/00/00/00/39); VERS, *Using digital signatures for authentication*, *VERS Version 1, Specification 3,* 1999.

The comparison of a digital signature with a seal does not hold up in several points. Someone's seal is the same for each document, whereas a digital signature is dependent on the content (bitstream) of a document. Different documents can have the same seal, but not the same digital signature. A seal is also directly associated with a legal person. With a digital signature, a legal person is linked to a private key. Finally, a seal is based on visual verification and a digital signature on invisible verification. The presence of a digital signature can be observed visually, but the actual verification is not visible.

9 H. MACNEIL, *Trusting records. Legal, historical and diplomatic perspectives*, Dordrecht, 2000, p. 108.

10 S. HUYDECOPER and S. VAN DER HOF, *De handtekening: van geschreven naar elektronisch* [The signature: from written to electronic], in: *Archiefbeheer in de praktijk*, 42, 1565.

11 H. MACNEIL, *Trusting records. Legal, historical, and Diplomatic perspectives*, Dordrecht, 2000; J. CURRALL, *Digital Signatures: not a solution, but simply a link in the process chain*, Glasgow, 2002, p.2 (http://eprints.lib.gla.ac.uk/documents/disk0/00/00/00/39).

Many extant solutions for the storage of private keys use smartcards, USB keys or network environments. In this last case the security is usually dependent on the ordinary checking of the user name and password.

The identity of a document is usually registered in the metadata of the document. File names, document profiles, attributes (author's name, date, place), classification codes, use within work processes, etc. are the customary methods for identifying digital documents. The identity of digital documents must also be protected against corruption. Unless the identifying metadata are encapsulated in the document itself, the digital signature does not check the identification of the document.

For the authentication of digital documents, digital signatures do not take into account the identity of the record. Making the authentication dependent on the bitstreams of digital objects, also ignores the fact that the same record can have various bit representations. In the concept of a digital signature, an electronic record is viewed purely as a digital object, whereas the same electronic record can be recorded as different digital objects. An e-mail with archival value can be preserved in various suitable archiving file formats (plain text, XML, PDF, TIFF, HTML). Depending on the file format in which a digital document is stored, the underlying bitstreams differ from each other. An electronic record cannot simply be equated with one bitstream or one bit representation.

Further, an authentication failure does not necessarily mean that the document is no longer reliable. Authentication with a digital signature will fail as soon as one bit of the computer file is modified. This does not automatically mean that the document is no longer authentic or has lost his integrity. The physical integrity (the bits) can be compromised, but the content can still be intact. Possible changes in the bits and bytes that do not involve a loss of authenticity are, for example, the encapsulation of metadata or bit degradation. To combine several items of metadata inextricably with the document, they are sometimes included in the same computer file as the document. An inadvertent 'falling over of bits' occurs more often than we may realise. RAID storage systems are specially provided for this, and in certain formats, error detection and error correction are abundantly applied.

3.3 Digital signatures prove the integrity of bitstreams

An advanced digital signature is an encrypted hash value of a computer file. With the validation function of a digital signature, it can be proved that after transmission the bits of a computer file are still the same as when it was signed. Each change after signing will result in an invalid document. The validation function indicates whether a document was changed during its transmission and/or whether the document was modified after signing. Digital signatures do not protect records from changes or manipulations.

The validation function of digital signatures is completely based on the bitstreams of which a computer file consists. The bitstreams can change while the content of a record has remained identical. With a digital signature, the bits of a computer file are signed and not the content of a record. Electronic records cannot simply be identified by means of one bit representation (one-to-one relationship). Rather, there is a one-to-many relationship between electronic records and bit representations (see 3.2).

By signing a document digitally, manipulations or corruptions are not prevented. The digital signature is a verification mechanism, not a protection or guarantee. If there is an invalid validation, it is not possible to discover by means of the digital signature what changes were made in the document after it was signed, by whom, or what the original content was. Yet, this is an important condition for an integrity guarantee for electronic records. After all, records do not loose their integrity when authorised persons make or carry out certain annotations. Thus, digital signatures cannot always demonstrate the integrity of electronic records. They only prove whether a digital object was, or was not, changed after it was signed.

Manipulations or changes can better be prevented by means of a digital signature if the sender encrypts the document with the public key of the receiver and then adds his own digital signature to the

document. In general, however, the international archival community rejects the archiving of encrypted documents[12]. Encryption conflicts with the principle of limiting the necessary chains in the reconstruction process. Encrypted records are therefore first decrypted before they are ingested in the digital repository.

3.4 Conclusion

From the above it is evident that, from a purely archival point of view, digital signatures are not a suitable method for proving the authenticity and integrity of electronic records. In the area of authenticity, digital signatures say nothing about the identity of electronic records. The authentication declaration does not extend beyond a proof that the document was signed by something/someone in possession of the private key of the signer. With regard to integrity, a digital signature only proves that the bits of the transmitted document are intact. Digital signatures do not prevent corruptions or unallowed manipulations.

As a consequence, it makes little sense for the records manager or the archivist to provide all electronic records with his digital signature. The archiving of authentic and integral records is more a question of the registration of essential identifying metadata, the description of records and taking of measures to guarantee the reliability of records (prevent changes, maintain an audit trail, documenting record-keeping actions, etc.).

4. THE LONG-TERM ARCHIVING OF DIGITALLY SIGNED RECORDS

From an archival point of view, archiving digital signatures is not sufficient to establish the authenticity and integrity of electronic records. Yet, the archivist needs an archiving solution for digitally signed records. Creators will apply digital signature techniques to meet all kinds of judicial requirements and these documents are eligible for (medium) long-term archiving. From the (Belgian) judicial perspective, at the current moment it is indeed important that the original document, with its original digital signature, remains preserved.

4.1 Archival issues

Digital signatures are designed for checking the validity immediately after the transmission of a document. The transmission and the associated verification is limited in time. However, certain digitally signed documents are eligible for (medium) long-term archiving and their authenticity must remain guaranteed just as long. The validation of electronic records by means of a digital signature at a time in the distant future may not be taken for granted, however:

- digital signatures are time-bound

[12] The Library and Archives of Canada rejects the archiving of encrypted messages for two reasons. Firstly, encryption has the function of an envelop. Envelops are not an integral part of the record and are not selected for preservation in general. Secondly, for the reconstruction of encrypted records the corresponding decryption key is necessary, which is an additional reconstruction dependency. On loss of the decryption key, the record must be considered lost (http://www.collectionscanada.ca/06/0618_e.html). Nor does the National Archives of Australia archive encrypted documents. In addition to the argument of the extra reconstruction dependency, the National Archives also refers to the fact that after receipt, the encryption no longer makes any sense. Encryption has after all as its initial purpose the protection of the content during transmission (NATIONAL ARCHIVES OF AUSTRALIA, *GDA for encrypted records created in online security processes*, May 2004).

- the bitstreams of electronic records might be migrated
- the validation chain must remain available.

4.1.1 DIGITAL SIGNATURES ARE TIME-BOUND

Whereas digital documents are eligible for a (medium) long or even permanent retention period, the digital signature technique is designed for the short-term validation of digital documents. Digital signatures are intended for the validation of documents immediately after transfer. In the PKI model, the transmission time is of short duration and certainly not commensurate with the medium long or long-term storage of electronic records. The authentication function of digital signatures has a short life-cycle. The validation of documents, after a certain time has elapsed since receipt, forms a problem for two reasons.

Digital signatures are a solution that is predominantly based on technology. Just like other technologies, authentication technology is subject to technological obsolescence. The hashing of bitstreams and the encryption of the hash code depends on specific algorithms and software. Both are subject to technological obsolescence, but are necessary for future (re)validation of digital signatures. A realistic expectation is that with the break-through of quantum computing the present algorithms will be consigned to the waste basket. It is already clear that key lengths must evolve along with the power of computers[13]. Powerful computers are getting faster and faster at cracking hash and encryption algorithms. For example, in 2004 Chinese researchers turned the cryptography world upside-down by announcing that the MD5-algorime is not so infallible[14].

Also, the certificates that are issued have a limited lifespan. Each certificate has a validity period that is limited in time. That validity period can in theory be no longer than the period during which the certification authority retains information about the public key. In practice, the validity period is limited to several years or even less because of the security of the keys and the algorithms. Digital certificates can also be revoked earlier (for example, on theft of the private key). The preservation period of records can exceed this validity period so that authentication by means of a digital signature forms a problem.

4.1.2 MIGRATION OF THE BITSTREAMS OF ELECTRONIC RECORDS

If authentication already presents problems when a bitstream is not intact, then such will certainly be the case when records are migrated to solve the problem of technological obsolescence.

The archival community has been working for more than a decade on the question of how electronic records can remain readable in the long term. Archivists agree in general that archiving on paper, conversion or building computer museums are not viable solutions for the long term preservation of electronic records. Migration of the records and emulation of the necessary hardware and software environment are the most cited digital preservation strategies.

---

[13] Thus the National Institute of Standards and Technology (NIST) advises against the use of MD5 (Message Digest 5, 128 bits) for digital signatures and certificates. The NIST also formulated the recommendation that SHA-1 (Secure Hash Algorithm, 160 bits) be replaced by 2010 by SHA-256 and SHA-512. (B.BURR, *Implications of recent analytic results hash functions: practical implications of recent analytic results*, at the Federal PKI Technical Working Group Meeting, 23 November 2004
(http://csrc.nist.gov/pki/twg/y2004/Presentations/twg-04-14.pdf)

[14] The researchers announced that they had found a so-called 'hash collision' (two different inputs that result in the same hash code) in MD5 (X. WANG ea., *Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD*, August 2004. (http://eprint.iacr.org/2004/199.pdf).

Migration is at present the most widely applied preservation strategy. The digital documents are migrated to a suitable archiving format. Standardisation of the file format is one of the most important requirements for such a suitable archiving format. For the time being, emulation is mainly a theoretical solution for the durability problem. It not only remains an open question whether emulation is a feasible track to follow, but it also appears very unlikely that emulation is an attainable solution for documents in proprietary and non-documented file formats such as the popular formats of the MS-Office package. For the construction of an emulator, one must have the specification of the format. In the case of a lot of proprietary file formats, the specification is not available and methods such as decompiling or reverse-engineering, that might be able to provide a (partial?) solution for this, violate copyright[15]. For this reason, in the emulation strategy, documents that are in closed file formats will probably first be migrated to a standardised file format. Subsequently, on the basis of the available format specifications, an emulator for consultation can be constructed.

The migration of digital documents to a standardised format has the consequence that the bits and bytes of the document are changed. The bitstreams that form the source and the target file, differ from each other and will produce different hash codes. After migration, the digital signature that was calculated on the source file will not be usable for the validation of the target files.

4.1.3 THE VALIDATION CHAIN MUST REMAIN AVAILABLE

To continue using digital signatures for the authentication of digital documents in the future, it is not sufficient to preserve the documents and the digital signatures alone. For verification, an external PKI structure is required. The complete 'validation chain' including the digital certificates and root certificates must remain available[16].

In the PKI model, certification authorities distribute the digital certificates. For the verification of digital signatures, these certificates must remain available. Certification authorities are usually commercial organisations. One has no guarantee that digital certificates will be preserved in the long term. Also, all software for the decryption of digital signatures and the hashing of digital documents would have to remain operational. Taking into consideration the relatively short lifespan of software applications, there is no evidence that the authentication technology will remain available. The reconstruction of the necessary software in the future on the basis of documented algorithms is indeed possible, but that would be a fairly expensive and complex issue. As soon as an essential part is no longer present or operational, the validation chain breaks.

The maintenance of such an external validation structure also conflicts with the archival principle that digital archives must be as self-sufficient as possible. All essential elements of the 'validation chain' must therefore also be present in the digital repository itself. Within the digital repository, a certificate archive would have to be set up. This certificate archive would have to be secured very well, so certificates could not be changed or added. Since certificates can expire or be revoked, it is also important that information about the status of the certificate be maintained (for example, the validity period, date and time the document was signed, certificate revocation list). The archiving of a time-stamp is important to show that a document was signed with a private key before the digital certificate expired or was revoked.

---

[15] F. BOUDREZ, *B. Preservation strategies*, in: F. BOUDREZ and H. DEKEYSER, *Digitaal archiefbeheer in de praktijk. Een handboek.* [Digital archive management in practice. A manual], Antwerp-Leuven, 2004.

[16] J. DUMORTIER and S. VAN DEN EYNDE, *Electronic signatures and trusted archival services*, in: Proceedings of the DLM Forum 2002, Barcelona 6-8 May 2002, Luxembourg, 2002, p. 520-524.

4.2 Solutions for long-term archiving

The problems of long-term archiving of digitally signed documents is at present still a research topic. The archiving of digitally signed documents and the associated digital signatures is not a problem in itself, but the verification of the digital signature in combination with ensuring the accessibility of the document is a problem. It is notable that several initiatives do offer a solution for long-term archiving of the digital signature and the validation chain, but not for the long-term consultation of the signed documents themselves[17]. The challenge, when archiving digitally signed documents, is precisely the finding of a suitable solution for both problems together. Tracks that are being investigated for this at present are:

- the re-signing of documents after migration
- the registration of the validation
- the preservation of the original bitstream and the validation chain
- the certification of the migration process

4.2.1 RE-SIGNING AFTER MIGRATION

Digital signatures loose their authentication function when electronic records are migrated to a different file format. After migration, the bits of the computer file are changed so that any validation after migration will result in differing hash values, and as a consequence the authentication based on the digital signature on the original document will fail.

A solution for this problem could possibly be the re-signing of the migrated documents[18], but this runs into both judicial and practical objections. The original signer can refuse to sign a document again or can have died in the meantime. The re-signing of the documents by a trusted third party could be a solution for this[19], but still conflicts with the legal point of view that a document may not be re-signed but that the "original" signature is necessary[20]. Furthermore, the declaration of a trusted third party does not have the same status as a personal authentication such as the advanced digital signature[21].

4.2.2 REGISTRATION OF THE VALIDATION

Immediately after receipt, the validity of the digitally signed document is checked by means of the digital signature. The result of this validation is registered by the receiver in the metadata of the

[17] Examples of this are: XML Advanced Electronic Signatures (XAdES); EESSI, *Electronic signatures and infrastructures (ESI)*; *Electronic signature formats (ETSI TS 101 733 V1.5.1 (2003-12))*, December 2003; D. LEKKAS and D. GRITZALIS, *Cumulative notarization for long-term preservation of digital signatures*, [without date] (http://www.syros.aegean.gr/users/lekkas/pubs/j/2004COMPSEC.pdf).

[18] C. LYNCH, *Canonicalization: a fundamental tool to facilitate preservation and management of digital information*, in: *D-Lib Magazine*, September 1999, (http://www.dlib.org/dlib/september99/09lynch.html); J. CURRALL, *Digital Signatures: not a solution, but simply a link in the process chain*, Glasgow, 2002, p.9 (http://eprints.lib.gla.ac.uk/documents/disk0/00/00/00/39).

[19] Such a solution was suggested in the draft text US FDA E.A. *Guidance for Industry 21 CFR Part 11; Electronic Records; Electronic Signatures: Maintenance of Electronic Records*, July 2002, p. 21 In the meantime this text has been revoked (for this, see US FDA E.A., *Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application*, 2003, p. 2-3).

[20] DEKEYSER, H. and DUMORTIER, J., *Juridische obstakels voor de elektronische handel op het vlak van archivering en datering*, Study commissioned by the FOD Economie, KMO, Middenstand en Energie, September 2004, unpublished, p. 26.

[21] J. DUMORTIER and S. VAN DEN EYNDE, *Electronic signatures and trusted archival services*, in: Proceedings of the DLM Forum 2002, Barcelona 6-8 May 2002, Luxembourg, 2002, p. 520-524.

document. These metadata must be archived together with the record and must be protected against manipulations or changes.

The underlying philosophy of this approach is that the authentication technology of a digital signature is predominantly a technological solution and does not escape technological obsolescence. Furthermore, the complete validation chain must be archived. An alternative is being sought in the embedding measures for establishing the authenticity and integrity in a procedure that is transferable in the long term and in which various technologies could follow each other. This approach also corresponds with the archival view that documents used within a work process are authentic, even though they have undergone changes[22].

The National Archives of Finland uses this approach and even goes a step further by not archiving the digital signatures. Also, the Netherlands standard for records management applications (ReMaNo)[23] and the NARA, provide this possibility[24]. It has been assumed that the preservation of digital signatures after verification, registration and inclusion of the document and its metadata in a reliable digital repository no longer has any value[25]. Furthermore, digital signatures become unusable after migration. The Finish approach is comparable with cutting off the signature at the bottom of a document and runs into judicial and archival objections. For judicial reasons, the original signature must sometimes remain preserved[26]. In the diplomatic area and in archival science, the signature at the bottom of a document is an extrinsic element of the documentary form that is usually viewed as “essential” and must therefore also be archived.

4.2.3 PRESERVATION OF THE ORIGINAL BITSTREAM AND THE VALIDATION CHAIN

Several initiatives seek solutions for the archiving of the validation chain so validation remains possible in the long term. For this it is not only necessary that the original bitstreams are archived but also all elements of the public key infrastructure that are necessary for verification after a certain period of time, such as the digital signature, the digital certificate with the public key, metadata about the certificate, time-stamp, counter-signatures, etc. The validation chain must be preserved and remain operational just as long as the signed documents are preserved. For each digital signature, as a minimum, the following information must be registered:

- the hashing algorithm used
- the algorithm used to calculate the digital signature
- the name of the signer
- the decrypted digital signature
- the public key
- the status of the digital certificate

---

22 INTERPARES AUTHENTICITY TASK FORCE, *Requirements for assessing and maintaining the authenticity of electronic records*, in: InterPARES, *The long-term preservation of authentic electronic records: findings of the InterPARES project*, 2002, p.2.

23 G.J. VAN BUSSEL, P.J. HORSMAN, H. WAALWIJK, *Softwarespecificaties voor Records Management Applicaties voor de Nederlandse Overheid* [Software specifications for Records Management Applications for the Netherlands Government], Amsterdam, 2004, p. 78-79.(http://www.archiefschool.nl/docs/ReMANO_2004.pdf).

24 NARA, *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*, Washington, October 2000, p. 13. A requirement of the NARA for digitally signed records with a permanent preservation period is that the name of the signer and the date of signing must be included in readable form in the record.

(http://www.archives.gov/records_management/policy_and_guidance/electronic_signature_technology.html)

25 R.POHJOLA, *Implications of electronic signatures - the situation in Finland*, at the *DLM FORUM 2002*, Barcelona, 7 May 2002.

26 J. DUMORTIER AND S. VAN DEN EYNDE, *Electronic signatures and trusted archival services*, in: Proceedings of the DLM Forum 2002, Barcelona 6-8 May 2002, Luxembourg, 2002, p. 520-524.

EESSI (European Electronic Signature Standardisation Initiative) developed a format with the name ES-A (Archival Electronic Signature) that has as its purpose the long-term verification of digital signatures[27]. XAdES or XML Advanced Electronic Signatures demonstrates many similarities to this approach. XAdES has the ambition of developing into an archiving format for digital signatures based on XML. XAdES is an expansion of the XMLDSIG Recommendation and offers various schemes for the storage of a digital signature and all essential metadata[28].

The VERS archiving strategy also provides for the archiving of all elements of the validation chain. The digital signature and all necessary certificates are encapsulated in containerfiles in which the records are packed (<SignatureBlock> in VEO objects). The VERS VEO containerfiles can contain both the original and the migrated bitstream of the records. The original digital signature and all dependencies can be included with the original bitstream. The migrated bitstream is signed digitally by the 'notary' or the record-keeping system[29]. Because of the low penetration of PKI, at the present time there is not yet a single practical implementation of the VERS archiving strategy in which the original digital signature is encapsulated in the VEO object. Thus in practice, the VERS archiving strategy is more of an application for re-signing after migration, but the theoretical model provides place for the preservation of the original digital signatures and the validation chain.

The application of this approach for the long-term validation of digital signatures has a number of practical consequences. Firstly, when validating digitally signed documents, the records management system of the creator must also preserve all digital certificates and associated metadata. This requirement is included, for example, in the Model Requirements for the management of electronic records (Moreq, 10.5.7) and in ReMaNO (requirement no. 261). Secondly, this solution is based on the archiving of the original digital objects. How the electronic records can be reconstructed on screen from those original digital objects in the long term, is still not clear. Advocates of this solution suggest emulation as a digital preservation strategy, but it is still an open question whether emulation is a practical or even sustainable solution. Also, the limitation of this solution to records in an open or suitable archiving format for which viewers can be created later, does not appear very realistic. The same applies for the signing of records in a “canonical form”[30]. One can not always obligate a signer to use a certain format. Migration will probably come to the fore as part of the solution for long-term consultation. The VERS archiving strategy, for example, provides for a migration of the records to PDF. And finally, a solution also needs to be elaborated for keeping the authentication technology itself operational in the future.

4.2.4 CERTIFICATION OF THE MIGRATION PROCESS

Another solution for the validation problem that exists after migration could be certification of the migration process[31]. In this case the migrated records are not re-signed. A trusted third party authorised to do so:

- verifies the digitally signed documents before the migration
- checks the migration process (audits the migration procedure, the software used, and the migrated records)
- supplies a certificate.

---

[27] ESSI, *Electronic signatures and infrastructures (ESI)*; *Electronic signature formats (ETSI TS 101 733 V1.5.1 (2003-12))*, December 2003.

[28] http://www.w3.org/TR/2003/NOTE-XAdES-20030220; A. EGGER, *Digitale Signaturen, Probleme und Lösungen bei der Archivierung* [Digital Signatures, Problems and Solutions in Archiving], December 2003.

[29] http://www.prov.vic.gov.au/vers/standard/advice_12/5-2.htm

[30] C. LYNCH, *Canonicalization: a fundamental tool to facilitate preservation and management of digital information*, in: *D-Lib Magazine*, September 1999, (http://www.dlib.org/dlib/september99/09lynch.html); W3C, *Canonical XML version 1.0*, Recommendation, 15 March 2001.

[31] RLG*, Trusted digital repositories: attributes and responsibilities*, Mountain View, 2002, p. 33-35.

This approach means that the reliability of the converted electronic records is no longer shown by means of a digital signature, but with a certificate. The migrated electronic records must be safeguarded against wrongful manipulations or changes.

4.3 Conclusion

The long-term archiving of a digital signature causes few or no problems. The archiving of the validation function, on the other hand, does require special attention. This results from the fact that digital signatures are not designed to validate digital documents in the long term. The solutions for the readability problem of electronic records increase this problem even more.

The separate solutions do not meet the judicial and archival requirements. The re-signing of records after migration must be rejected from a judicial perspective. The removal of the digital signature after validation is usually not allowed judicially or according to archival science. The metadata of the validation process that must be archived together with the record itself are important from an administrative, judicial and archival point of view. The preservation of the original bitstreams, the digital signature and the validation metadata becomes a necessity.

Further research must reveal whether it is sufficient to preserve the digital signature and the validation metadata or whether it is actually necessary for the validation function and the associated software to be archived as well. This last option is technically the most complex. Both archiving solutions can also be used besided each other For digitally signed records with a limited retention period, one could preserve the validation chain and keep it operational, whereas for records with a permanent retention period the validation metadata and a reliable records management system could take over the role of the digital signature. The National Archives of Australia leaves both possibilities open and suggests that an approach be chosen on the basis of a risk analysis, and not on the basis of the retention period. According to the National Archives of Australia it is not likely that digitally signed records still can be validated with digital signatures after their transfer to the archives[32].

It therefore appears that a solution for the preservation of digitally signed documents will consist of a combination of the remaining solutions such as the archiving of the original document and the validation chain, on one hand, and making (certified) copies for consultation purposes (migration), on the other hand. The digital preservation strategy of the DAVID project takes this into account by including both the original and the migrated bitstream in the digital repository. Whether certification by a trusted third party will be necessary depends on the confidence that one has in the archivist, the records management system of the creator or the record-keeping system of the archival service. External certification of the migration process and/or of the migrated records can only increase the trust and the reliability[33]. One can also ask oneself if making certified copies is not the most that is attainable. After all, in the digital world, what is stored (bits & bytes) and the record in an intelligible form are not the same and each consultation results in the creation of a new copy. Electronic records are actually by definition reproductions of originals, even though one consults a digital document in its original file format. An important point for consideration in the demonstration of the authenticity is the proving or referencing of the status of the copy in relation to the original[34].

---

[32] NATIONAL ARCHIVES OF AUSTRALIA, *Record keeping and online security process: guidelines for managing commonwealth records created or received using authentication or encryption*, Canberra, 2004. (http://www.naa.gov.au/recordkeeping/er/security.html). The National Archives do not archive the public keys or digital certificates themselves but do allow the creator to keep all elements of the validation chain up to date himself.

[33] R. DALE, *Certification and audit*, at the Erpa Workshop *'Trusted digital repositories for cultural heritage'*, Rome, 17-19 November 2003.

[34] INTERPARES AUTHENTICITY TASK FORCE, *Requirements for assessing and maintaining the authenticity of electronic records*, in: INTERPARES, *The long-term preservation of authentic electronic records: findings of the*

Regardless which solution is selected for archiving digitally signed documents, the archivist must provide for an record-keeping system that is able to transfer authentic and integer records in time. After all, digital signatures do not prevent manipulations or changes. Furthermore, the digitally signed records will only constitute a minority of all electronic records that the archivist preserves. The authenticity and integrity of the non-signed electronic records need to be guaranteed just as well.

5. GENERAL CONCLUSION

The use of an advanced digital signature as a proof of authenticity and integrity for electronic records raises several questions and problems. They result in particular from the fact that the whole concept of the digital signature is based on a digital object. This ignores the fact that electronic records are much more than just digital objects or original bitstreams. When trying to find reliability guarantees for electronic records, one must start with the concept of the electronic record, and not that of the digital object. Otherwise the danger is great that the *recordness* of electronic records will be lost or that measures must be applied that run counter to the reconstruction process that lies at the base of digital preservation.

The measures or guarantees for establishing the reliability of electronic records must also be transferable in time. The problems regarding to the long-term validation of digital signatures are inherent in the whole concept of the digital signature. In addition to the dependence on a 'validation chain', there is also a huge dependence on technology (reconstruction of the record, hashing, calculating the digital signature, encryption, etc.). Technology becomes obsolete quickly and therefore may not be the exclusive basis for assurance of reliability. Technological solutions must be replaceable and must be embedded in an overall management procedure.

Furthermore, one may not forget that reliability includes more than authenticity and integrity alone. Accuracy and trust also play an important role in the archiving of reliable records. Assurance of reliability is a never ending process that starts on creation or receipt, and must be maintained during the entire life cycle.

InterPARES project, 2002, p.4.