Electronic Signatures and Trusted Archival Services

Jos Dumortier & Sofie Van den Eynde
K.U.Leuven – ICRI

I. INTRODUCTION

Recent legislation on a European level has abolished some of the legal barriers regarding electronic document creation and preservation. The European Directive 1999/93/EC ¹ deals with electronic signatures. Where the use of electronic documents is legally permitted, so-called “qualified electronic signatures” must receive a status that is equivalent to the legal status that handwritten signatures normally have in relation to paper documents. Furthermore, the Electronic Commerce Directive ² obliges the Member States to ensure that the legal requirements applicable to the contractual process (the archival phase included!) neither create obstacles for the use of electronic contracts, nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means. Legal rules enforcing the use of paper documents in the contractual process must be progressively abrogated. Consequently, a lot of important documents, that are now still mostly paper-based, such as contracts and other legal instruments, will in the future solely exist in their original electronic form. It is needless to say that this evolution could lead to an increasing need for electronic archival services.

The PKI-based technique of the digital signature plays an important role in this new legal framework. From the current state of the law in Europe results that only PKI-based digital signatures can bring forth so-called “qualified” electronic signatures. The digital signature technique allows authenticating electronic information in a way that the origin of the information, as well as its integrity can be verified. A digital signature is an encrypted hash-code that is deduced from and attached to the electronic information that has to be authenticated. If only one bit changes over time, the verifier of the digital signature will notice that the integrity has been affected. The verifier can also be sure that the electronic information originates form the signatory, since he is the only one who knows his own private key.

As a result of this new legal framework, archivists are increasingly challenged to deal with digital signatures as an organic part of electronic documents. However, there exists a lot of resistance in the

archival community against the preservation of digital signatures. This is well-illustrated by the report of the InterPares Authenticity Task Force, entrusted with the task of identifying “conceptual requirements for assessing and maintaining the authenticity of electronic records.” The Task Force adopted an unequivocal position with regard of the role of digital signature technologies and PKI as a means of ensuring the authenticity of records:

“Digital signature and public key infrastructure (PKI) are examples of technologies that have been developed and implemented as a means of authentication for electronic records that are transmitted across space. Although record-keepers and information technology personnel place their trust in authentication technologies to ensure the authenticity of records, these technologies were never intended to be, and are not currently viable as a means of ensuring the authenticity of electronic records over time.”

In this paper we will first investigate the need for electronic signatures to be verifiable years later from a legal point of view. We will also focus on several standardization initiatives that were launched by the European Commission within the framework of the European ICT Standardization Board regarding long term validation and long term archival of digital signatures. This analysis will draw the attention to the fact that digital signatures can be archived with the expertise and the stability epitomized in a Trusted Archival Service. To conclude, this paper will instigate the establishment of a legal framework for this kind of trust services.

II. ELECTRONIC SIGNATURES, DIGITAL SIGNATURES AND PUBLIC KEY ENCRYPTION

Although digital signatures are known best as a substitute for handwritten signatures with legal value (= electronic signatures), the technique of the digital signature has many other applications. It can be used in all cases where the origin and the integrity of electronic data have to be guaranteed. These

3 J.P Blanchette, ‘Dematerializing’ Written Proof: French Evidence Law, Cryptography and the Global Politics of Authenticity, Doctoral Dissertation submitted to the Department of Science and Technology of the Rensselaer Polytechnic Institute, 2001, p.308, writes: “The fundamental premise of the InterPARES project is that authenticity is not primarily a function of technology, but rather, of institutions. Archivists have historically been entrusted with the task of providing this function, within either private or public institutions, and they remain the most appropriate, professionally organized, socially recognized, historically legitimate profession to accomplish similar functions in the electronic environment.” The interesting dissertation of J.P. Blanchette is available at http://www.rpi.edu/~blanc/thesis.pdf

4 See the draft final report of the InterPARES Authenticity Task Force, http://www.interpares.org/documents/atf_draft_final_report.pdf, p. 8

5 The possible use of digital signatures for the preservation and authentication of records through time has been analyzed in the framework of the DAVID-project (which stands for Digital Archiving in Flemish Administrations and Institutions, http://www.antwerpen.be/david). See also: VAN DEN EYNDE, S., The OAIS Reference Model as starting point in search of the role of Public Key Infrastructure for electronic archives, Leuven, Interdisciplinary Centre for Law and Information Technology, August 2001, 63 p. (in Dutch only).
qualities are very important for documents that are stored in archives. A digital signature added to the (signed) record by the archivist, allows the verifier of the signature to check the identity and the authority of the archivist. That is how the authenticity of a record “as a record” can be checked in a network environment. The presence of the digital signature of the archivist in the metadata of a record indicates that that record has the status of an archived record. The use of the digital signature technique also creates the opportunity for checking the integrity of electronic records. When used in this manner, the digital signature functions as a “seal”. 6 By creating and archiving an encrypted, and thus inaccessible hash code, it can be noticed at all times when the plain text has been tampered with.

It is true that PKI-based digital signatures have been considered for a while as an essential tool for archival purposes. It has been argued that all electronic data should be secured with digital signatures before entering the archive. The integrity of the electronic data stored in the archive could then, in this view, be controlled by the verification of the archivists’ signature.

Skepticism about this theory appeared as soon as it became clear that, when using digital signatures, control of the integrity is only possible if the electronic data remain completely unchanged at the bit-level. This raises a problem when archivists want to migrate electronic data to new formats or software platforms in order to keep them accessible and legible. Some people have immediately concluded that digital signatures are therefore not useful and hence not relevant for archival purposes. If a digital signature secures a document before it enters the archive, the signature should be stripped and translated into metadata.

From a legal point of view however, in order for signed documents to keep their value over time, it is often important that the original electronic signature is still present. Signatures can be needed for non-repudiation purposes in an evidential context, for example. Many European countries require for proof that non-commercial transactions are embodied in a signed document. 7 Recent developments in the context of e-government have also made clear that signed electronic communication with the government must be archived. The government who picks the lowest bidding firm in the context of a public contract conducted by electronic means, will want to be able to proof before court that this firm is bound by its price offer.

The content of the document and the signature are one indivisible artefact in the paper world. A traditional signature has all the characteristics of a classical one-way function: it is easy to process in one direction but very difficult to reverse the process, i.e. the signature is easy to affix but difficult to remove. This is not the case with electronic signatures: an electronically signed document is not different from an electronic document that has not been signed except that it has appended to it another series of bits that can be used to identify the signatory and verify the integrity of the document. Thus,

---

6 As opposed to the digital signature used as an electronic signature with legal value in the sense of the European e-Signature Directive.

an electronic signature can very easily be stripped from a document for fraudulent purposes without leaving a trace.

Although they have the same functions from a legal viewpoint, traditional signatures and electronic signatures are two very different concepts that need to be treated differently. Never before in the history of written communication a signatory has had to worry about how the signature will be linked to the content of the document that he is signing. When using electronic signatures, this becomes now a very relevant issue. The content of the document and the digital signature should be concatenated and the hash-code of the concatenation should be lodged with an independent entity that will time stamp the hash-code. The hash-code establishes the bond between signature and content. The time stamp must be included in the metadata of the document. The intervening independent entity is designated in this paper by the term “trusted archival service”.

III. LONG TERM VALIDATION OF ELECTRONIC SIGNATURES

The European Commission took the view that the requirements identified by the e-Signature Directive needed to be supported by detailed standards and open specifications so that products and services supporting electronic signatures can be known to provide legally valid signatures. A mandate was issued to European standardization bodies, CEN/ISSS and ETSI, to analyse the future needs for standardization activities. Under the auspices of the European ICT Standardization Board the European Electronic Signature Standardization Initiative (EESSI) was launched. The first result of this initiative was an expert report about future standardization requirements. This report affirms that trusted archival services could play an important role in supporting electronic signatures that may need to be used in evidence long after they were created and identifies it as a topic requiring further study since no standards exist yet for the use of such services in support of electronic signatures. In the mean time, ETSI has published a standard “Electronic Signature Formats” defining all the elements necessary to prove the validity of a signature long after the normal lifetime of the critical elements of an electronic signature. This so-called validation chain has to be archived.

Thus, it is not enough that just the electronic signature and the content of the document are present in the archives when a signed document is needed years later. In order to perform validation, the certificate used by the signatory must be obtained, and its validity at the time of signature creation must be proofed. It is possible that the certificate was valid at the time of signature creation, but had expired or had been revoked or suspended some time later. By consequence, the certificate status

---


10 Electronic Signature Formats, ETSI TS 101 733 v.1.3.1 (2002-02).
information must be archived as well. Signature validation must be performed immediately after, or at least as soon as possible after signature creation time, and not only at archival time, in order to obtain certificate status information that was issued by the CA as closely as possible to the moment of signature creation.

Only the moment of signature creation has an archival value. A signature that has been found to be valid at signature creation time shall continue to be so for the same document months or years later. Evidence must be provided that the document was signed before the certificate became invalid. Thus, the time of signature creation must also be determined and archived. A time stamp can provide for such evidence. A time stamp is a set of computer data, consisting of the hash code of the digital signature and the time of stamping, signed by a Time Stamping Authority (TSA). It proves that the digital signature was formed before the certificate became invalid. Anyone who wants to make sure that he can rely on a signed electronic document for proof years later, must obtain a time stamp before the certificate becomes invalid. The sooner after signature creation time the time stamp is obtained, the better it is for legal certainty.

IV. LONG TERM ARCHIVAL OF ELECTRONIC SIGNATURES

The availability in the archives of a complete validation chain is a necessary, but not the only condition to make long term signature validation possible. In the end, all we can preserve in an electronic context are bits. However, it has been clear for a long time that it is very difficult to keep a set of bits indefinitely. With the lapse of time, the set of bits becomes illegible (to the computer and thus to humans) as a result of the technological obsolescence of the application program and/or of the hardware (e.g. the reader). This paradox causes difficulties for the long-term validation of electronic signatures. Every alteration to the record after signature creation time will make signature validation fail. Reformatting operations that must keep a record legible for the future (such as migration, conversion) are thus detrimental to the durability of the signature.

The problem of the durability of PKI-based digital signatures has been poorly studied so far because of its complexity. Still, some solutions are found in literature, mostly coming from the industrial community. It should be mentioned that we are confronted here with a unique problem from a historical perspective. Although the authentication tools that were used in the past, such as handwritten signatures, seals, stamps, fingerprints etc. are also subject to reformatting (e.g. microfilming) because of the obsolescence of the paper carrier, they never become completely useless after reformatting. There is always at least a copy available that can be compared with other original authentication tools.

It is the responsibility of each Certification Authority (CA) to make available in repositories on the Internet all the information needed to validate any signature that was created by means of a certificate issued by that CA. This includes making public at a regular basis information about the time a certificate expired, or was revoked or suspended.
The original signatory may resign the reformatted record with his private key. This solution is of course unimaginable from a legal viewpoint. A person cannot resign a document, as it would be a totally new document with the same content however, but signed at a later date. Furthermore, a signatory could refuse to sign, or if he could have deceased.

Another option would be to strip the digital signature, or in other words not to archive the digital signature. A trusted third party could certify that the original signatory signed a previous version of the reformatted record, but which is identical with respect to the content. In this scenario the digital signature is not archived along with the reformatted record as it is cut off as soon as the record is subjected to reformatting. However, this solution puts up legal and practical barriers. A signature is an utmost personal authentication tool, which can never be replaced by a declaration of a trusted third person. Such a record has at best the value of a certified copy. Current legislation in many European countries still requires the submission of an original record though. Furthermore, in a network environment one can never proof the identity of the trusted third party who certified the existence of the signature, without using digital signatures. This is the same problem of a certification authority that certifies the identity of the signatory in a certificate. In order for the public to trust that certification authority, the certificate must be signed by the certification authority with its own private key. A trusted third party that certifies the existence of a signature e.g. in the metadata (the metadata have the same function here as the certificate in a PKI), must create the opportunity for the public (e.g. the participants in the archival network) to believe the metadata. Therefore, one will want to know the origin of the metadata. In the current state of technology, digital signatures are indispensable for this purpose. The problem of long-term authentication of the signatory is thus replaced by the problem of the authentication of the metadata.

The World Wide Web Consortium \(^\text{12}\) has also tried to formulate answers for the problem of signature-volatility. The W3C is responsible for the development of XML (eXtensible Markup Language), which is nowadays the most popular standard for structured information exchange. The XML 1.0 Recommendation defines multiple syntactic methods for expressing the same information. That is why XML applications tend to represent the same content in different ways. Therefore, XML “canonicalization” was designed.\(^\text{13}\) The canonicalization method uses an algorithm to generate the canonical form of a given XML document. The canonical form is the common denominator so to speak for all possible syntactic representations of a given content. A digital signature over the canonical form of an XML document allows the hash calculations to be oblivious to changes in the original document’s physical representation.

It would be naïve however to believe that XML signatures (namely a digital signature generated from a hash code over the canonical form of the XML document) will solve the problem of digital signatures becoming obsolete. To begin with, the canonicalization method developed for XML 1.0

\(^{12}\) http://www.w3c.org

\(^{13}\) Canonical XML, Version 1.0, W3C Recommendation, 15 March 2001

http://www.w3c.org/TR/2001/REC-xml-c14n-20010315
may not be applicable to future versions of XML without some modifications. The transfer of an XML document to this newer version will invalidate the signature, since the canonical form cannot be carried indefinitely into the future. At the moment, software companies are implementing XML in their products. The multiple use of XLM and its vendor independent character give XML the status of de facto standard. But it is not very likely that XML will be maintained as a common format forever. IT will keep evolving and it is unthinkable that there will never be a better alternative for XML. A canonical form that takes all current and future formats into account is unfortunately still IT science fiction.

The only effective solution in our view for the problem of signature durability, is the archival of the original binary representation of the document. This solution was proposed by the European Electronic Signature Standardization Initiative (EESSI) in the study report “Trusted Archival Services”. A TAS must guarantee that it will still be possible to validate an archived document years after the initial archival date, even if the applications that have been used at signature creation time are no longer in use. In other words, the TAS should maintain a set of applications (viewers as well as signature validation applications) together with the corresponding platforms (hardware, operating systems) or at least an emulator of such applications and/or environment in order to guarantee that the signature of the document can still be validated years later.

To achieve this goal in the best possible way, the TAS must only accept documents in a format that can still be understood when the format will no longer be in use. Only open file formats that are vendor-independent qualify for long term archival. Indeed, open file formats, such as XML are being so clearly delineated that the content of such documents should be legible even fifty years from now. For today’s undocumented, proprietary formats on the contrary (such as Microsoft’s Word), it is likely that it won’t even be possible to build emulators since no one besides the vendor has an insight in the syntax of these formats. Every TAS must therefore publish a list of supported document formats. Such a list may be exhaustive (for public services dedicated to a wide audience) or very restricted (for private services dedicated to very specific types of archival). Every time a document is submitted, the TAS must check the format before accepting it for archival.

The costs and expertise required for this solution, justifies that the task of archiving signed documents will be appointed to an independent third party such as a TAS. Although contractual freedom also applies for the manner in which contracts are archived, private persons will not always be able to securely keep signed documents in their own possession. Governments must ensure TASs to be introduced in their Public Key Infrastructure for archiving important governmental documents. Every community, from universities to notaries, from public authorities to businesses, must start thinking about how they will make use of a TAS in the future.

---

14 European Commission, August 2000, 37.
It is true that the emulation strategy fails to gain a lot of approval in the archival community. Therefore, we propose to organize TASs in accordance with a Decentralized Archival Model. In this model, the TAS is defined as a component of a distributed service and is only archiving signatures (and the original bitstream) while other generic archival services can remain responsible for archiving documents and keeping them legible. In this way, it is possible to reconcile signature durability and content readability.

V. A COMMON LEGAL FRAMEWORK FOR TRUSTED ARCHIVAL SERVICES

A TAS should be able to present and validate signed documents years after their initial date of archival. As it was already indicated in the final report of the EESSI expert team, standards must be developed for the use of trusted archival services in support of electronic signatures. A clear Community framework regarding the conditions applying to TASs will strengthen confidence in and general acceptance of electronic signatures. This new legal framework should determine:

- that Member States must ensure that by accepting a signed document for archival, a TAS is liable for damage caused to an entity or a legal or natural person who relies on the TAS for presenting the signature and the validation chain as regards the immediate and complete character of the presentation. Breach of this “obligation de résultat” should mean that liability is indisputable. A TAS should not be admitted to proof that he has not acted negligently since the loss of evidence is irreversible. Therefore, a TAS must obtain appropriate insurance to bear the risk of liability for damages.

- that there is a need for urgent standardization to determine which conditions must be fulfilled for a validation chain to be complete. The completeness of the validation chain determines the outcome of the validation process, and thus the legal effects of the signature.

- that the archives of a TAS can never be destroyed. For the case where a TAS ceases its activities, procedures must be drafted to steer the transfer of the archives to another TAS. In order to prohibit that a TAS goes into failure, a very strict investigation regarding the financial situation and prospects should be carried out prior to the start of his activities.

- that a TAS must employ personnel who possess the expert knowledge, experience and qualifications necessary for the archival services provided.

- that a TAS must use trustworthy systems to store the documents, the signatures and the validation chains so that only authorized persons can make entries and changes.

- that a TAS, before entering in a contractual relation with a person who wants to archive a document to support the signature, must inform that person of the precise terms and conditions of the storage, such as the term of storage and the accepted file formats. Such information, which may be transmitted electronically, must be in writing and in understandable language. Relevant

---

parts of this information must also be made available on request to third parties relying on the archived document for proof.

VI. CONCLUSION

It is clear that the archival of “qualified electronic signatures” was not taken into account when writing the e-Signature Directive. Art. 12 of the e-Signature Directive states that the European Commission shall review the operation of the Directive and report thereon to the European Parliament and to the Council by 19 July 2003 at the latest. The archival of digital signatures used as a substitute for handwritten signatures with legal value so that they are verifiable years later for non-repudiation purposes, is one of the issues that needs to be considered in this review. We believe that the establishment of a legal framework for Trusted Archival Services and the development of standards can take away the uncertainty that is prevalent in the archival community regarding the issue of digital signatures.