Preservation of Signed Electronic Records

Introduction

Imagine for a moment a judge trying to resolve a dispute between Alice, Bob and Carl in the year 2025. To prove their point, the parties invoke several records – for instance contracts – that were electronically signed by them in the year 2005. Before ruling on the merits of the case, the judge must first decide if the evidence presented is admissible in court and whether it carries any weight. For the parties involved, the time has come to bear the consequences of the preservation strategy they have chosen.

Carl opted for a hard copy strategy early on, even though this implies sacrificing certain elements of the records, notably electronic signatures. Alice has discarded all original signatures, replacing them with metadata created herself or provided by a a trusted third party. Bob has insisted on the use of qualified electronic signatures (QES) by all signatories and has made every effort to preserve them in a fully functional form.

In the next sections, a brief overview of the EU legal framework applicable to electronic signatures will be given, followed by an exploration of some preservation strategies for digitally signed records. Finally, an illustration will be given of how a Belgian judge would approach the different preservation strategies in a contractual dispute.

E-signature law in brief

In the EU a harmonized legal framework for electronic signatures is in place since a directive was issued on the subject in 1999.[1] The E-signature Directive defines various types of electronic signatures and attaches different legal consequences to each.

An electronic signature is any data in electronic form that is attached to or logically associated with other electronic data and serves as a method of authentication (Article 2, 1° E-signature Directive). For example, putting your name under an ordinary e-mail can be regarded as a very basic form of an electronic signature. Understandably, an electronic signature is not accorded much legal weight as such. Electronic signatures must be admitted as evidence in court and may not be dismissed just because of their electronic form (Article 5, §2 E-signature Directive). The judge remains free to dismiss an electronic signature on other grounds.

More weight is attached to a specific kind of electronic signatures, namely the advanced electronic signature (AES). Such a signature is uniquely linked to the signatory, is capable of identifying the signatory and is created using means under the sole control of the signatory. Also, it is linked to the signed record in such a manner that any tampering is detectable (Article 2, 2° E-signature Directive). In the current state of technology, only digital signature technology[2] can fulfill all these requirements. Oddly, the E-signature Directive defines this category of signatures without attaching any specific legal consequences to its use.

---

[1]Directive 1999/93/EC of the European Parliament and of the Council of December 13, 1999 on a Community framework for electronic signatures, Official Journal, January 19, 2000, L13/12 (hereafter E-signature Directive), available on <http://www.europa.eu.int/eur-lex/nl/index.html>. The member states were obligated to transpose the directive into national law by July 2001.

[2]In this paper the term 'digital signature' refers to signatures created using asymmetrical encryption.

A subset of advanced electronic signatures enjoys a particularly privileged status, specifically the AES which is accompanied by a qualified certificate and is created by a secure-signature-creation device. This subset is usually labeled a qualified electronic signature (QES) in legal literature. Not only must a QES be admissible as evidence in legal proceedings, it must be accorded the same legal consequences as a handwritten signature would receive in similar circumstances (Article 5, §1 E-signature Directive). The main benefit of using a QES over any other kind is the uniformity of its treatment in the entire EU. This property is very attractive to anyone seeking to maximize legal certainty. In a very limited number of cases, the use of a QES may be imposed by law, notably in the public sector.

Although the E-signature Directive is written in terms that are supposedly neutral towards the signature technologies available on the market, the conditions of an AES are tailored to digital signature technology. As of yet, the predominance of digital signatures remains unchallenged. For this reason, the rest of this paper will focus mainly on the preservation of digitally signed records.

In Belgium, the E-signature Directive has been transposed quite literally. The definitions of qualified, advanced and generic electronic signatures have been copied into Belgian law.[3] One difference with the directive is the fact that specific legal consequences are attached to the advanced electronic signature as well. An AES is a valid signature, as required on documentary evidence of a private agreement.[4] The roll out of the electronic identity card will give all Belgian citizens the means to create digital signatures. A reliable preservation strategy for signed digital records is needed urgently.

Preservation strategies for digitally signed records

Today, a number of strategies for the preservation of digital records – signed or unsigned – are on the table. There are also a few solutions targeted specifically at the preservation of digital signatures.[5] However, finding an appropriate solution for signed records as a whole is still a challenge.

Store in a cool dry place

In our example, Carl opts for a hard copy preservation strategy. Any signed records sent or received are printed to paper or micro-film and then archived. Arguments for this strategy are the durability of these media and their low-tech nature. Important drawbacks of this strategy are the high costs of storage, limited availability of the records and the amount of effort involved in reuse of information. Certain types of digital records cannot always be printed to paper in a meaningful way, e.g. video and sound recordings, databases, 3D environments, etc. Hash values, digital signatures and certificates can be printed, but cannot be used to authenticate paper records.[6]

---

[3]See the law of July 9, 2001 on a legal framework for electronic signatures and certification services, hereafter CSP Law (M.B. September 29, 2001).

[4]See article 1323 as amended by the Law of October 20, 2000, on the use of communication technology and the electronic signature in judicial and non-judicial proceedings (M.B. December 12, 2000).

[5]F. BOUDREZ, *Digital signatures and electronic records*, Antwerpen, eDavid, 2005, forthcoming, <http://www.edavid.be>; See J.-F. BLANCHETTE, *La conservation de la signature électronique: perspectives archivistiques,* Paris, La Documentation Française, 2004, 39 p.;

[6]In theory, the bitstream could be printed as well, though this appears rather pointless. The costs

Bob has insisted on the use of a QES by all signatories in order to benefit from its privileged status as a perfect substitute for a handwritten signature. In practice, this means using digital signature technology created with a secure signature creation device and accompanied by a qualified certificate. Subsequently, he has made every effort to preserve the signatures in a fully functional form. Bob captures and preserves the entire validation chain, complete with certificates and time stamps. For the signed records themselves, Bob opts for an emulation strategy.

Alice finds the preservation strategies chosen by Bob and Carl unappealing. She wants to archive her digital records in digital form and preserve the characteristics that are essential to her. Sound and video should remain playable, databases should remain browsable, and records should remain readable and stable. Alice decides not to preserve the digital signatures that served to authenticate her digital records. Instead, success or failure of signature validation is recorded in the record's metadata upon receipt. Before passing on migrated records to others, Alice may sign them. For records of great importance, a trusted third party may be involved to certify the migration procedure or the validation metadata.

Should it stay or should it go?

The greatest strength of digital signature technology – signaling manipulation of the bitstream – is also its greatest weakness. Validating a digital signature is only possible as long as the original bitstream remains perfectly intact. Achieving this, even for relatively short periods of time, is not as straightforward as it sounds. In most storage media, single bits 'falling over' is a rather common occurrence. Even in storage media specifically designed for this purpose, like CD-WORM disks, all reading equipment depends on built-in software to correct errors.[7] It is noteworthy that digital signature technology by itself does nothing to prevent any changes to a bitstream. Protecting bit integrity is a basic function provided by electronic record keepers.

Bit degradation affects Bob and Alice in differing ways. In Bob's case, the slightest change to a bitstream will break his digital signatures. In extremis, an irreparable modification of one single bit leads to the failure of his preservation strategy for the signed record in question. Faced with such failure, Bob could still try switching to Alice's strategy for the affected records, presuming that he recorded the validation results of the signatures as a precaution.
Alice will also prefer her bitstreams to remain intact, although slight modifications may be acceptable if the message conveyed remains unaltered. Clearly, this depends on the type of record. In case of a contract, a change in the amount of goods ordered from one hundred to one thousand items amounts to a breach of integrity. In contrast, a shift in one pixel in a video will probably not affect the message conveyed at all. Signaling integrity on the bit level is not the same as ensuring integrity on record level.

Bit degradation is not the only hurdle to take. A bitstream as such is not very useful. Without the necessary hardware and software to translate it into a record on a screen or in print, the content is inaccessible. In the past decades, hardware and software

---

involved in retyping the bitstream are prohibitive and OCR technology is currently not accurate enough. Disregarding these problems, the issue of translating the bitstream into an understandable record remains.

[7] F. BOUDREZ, CD's voor het Archief, Stadsarchief Antwerpen – ICRI K.U.Leuven, p. 10, available on <http://www.edavid.be/davidproject>. B. STARRET, 'Compact Disc Errors', in: Roxio CD-R Newsletter, April 21, 2000, available on <http://roxio.com/en/support/cdr/cderrors.html>.

platforms have come and gone at an alarmingly high rate. The file formats dependant on these platforms are at risk of becoming obsolete as a consequence. Records created in an open standard format are more or less immune to this problem. In all likelihood, this will only be the case for a fraction of Bob's and Alice's records. In the office environment, proprietary file formats abound. Even on the internet, which thanks its existence to open standards, strict adherence to the available standards is fairly uncommon.

Emulation is one way to deal with file format obsolescence. An emulator recreates the functions and behavior of the obsolete platform—meaning the old hardware, software or both—on a contemporary platform, allowing the original files to be accessed and used. This strategy allows Bob to present his original files as evidence when required. In this event, Bob can provide any accompanying digital signatures as well. At that point the signatures can be validated, if the specifications are available. If Bob has used proprietary digital signature technology, an emulator might be required just to validate the digital signatures.

In theory, emulation appears to be the ideal preservation strategy for signed records. Of course, things are not as simple in practice. Developing reliable emulators is a difficult and costly process, especially for platforms that are not fully documented. Witness to this is the limited number of emulators available today for obsolete platforms. On top of this, emulators developed to run on current platform will become obsolete in their turn. Over time, a chain of emulators must be built or replacements developed. Once the chain breaks and no replacements are forthcoming, all dependant records are lost.[8] The fact that the digital signature accompanying the file can still be validated offers little consolation.[9]

Migration is a second strategy to overcome file format obsolescence. Migration entails the transformation of a computer file into a suitable archival format. Some of the characteristics of the original file may be altered or lost in this process, depending on the specifics of the target format.[10] For Alice, migration is a perfectly viable option. Of course, she must use reliable migration tools and document the process in her records' metadata. In the end, she must be able to show that the migrated file and the original file essentially represent the same content.[11]

For Bob, migration is less attractive. The digital signatures accompanying the original file cannot be used to validate the migrated file, as this new file has its own distinct bitstream. After migration, Bob ends up with an unsigned file that is readable and with a signed file which is doomed to become unreadable. Under these circumstances, Bob must ask himself if keeping both files is really necessary.

As if bit degradation and file format obsolescence were not enough, there is still the issue of weakening encryption to address. The assumption underpinning digital signatures is that - with current available computer power - it just takes too long to

---

[8]BOUDREZ, F., DEKEYSER, H. and DUMORTIER, J., *Digital Archiving: The new challenge?*, Louvain-La-Neuve, I.R.I.S., 2005, pp. 83-84.

[9]Emulators have been successfully developed for various game consoles, but also for other computer systems, see <http://en.wikipedia.org/wiki/List_of_emulators>.

[10]For instance, when converting MS Word files to flat files, the original look and feel is lost; if the same MS Word files are migrated to uncompressed Tiff files, the original look and feel of the record is preserved, but the ability to reuse the content is lost instead.

[11]Transformation of signed documents in a legally secure way is the subject of a German research project called Transidoc, <http://www.transidoc.de>.

try all possible keys to crack the code. As time goes by, ever more powerful computers are developed, and such a brute force attack becomes a distinct possibility. For this reason, the length of encryption keys is increased regularly. Also, flaws may be found in the encryption or hash algorithm, opening up new avenues of attack.[12] New encryption algorithms are constantly under development, to replace broken ones. But longer keys or new algorithms don't solve the vulnerability of existing digital signatures. Once the key or the algorithm is broken, fake digital signatures - indistinguishable from genuine ones - can be created.

Alice is not confronted with this problem, as she discards the original signatures from her records. If she signs her records and metadata before presenting them as evidence, she can do this using state-of-the-art signature technology. Bob however must find a way to protect his old signatures. One obvious solution to the weakening of digital signatures, is re-signing old signatures with more recent technology.[13] From a technical point of view, this is certainly feasible, in practice though this scenario may prove very cumbersome.

One final consideration to take into account when comparing Alice's and Bob's strategy is the fact that a digital signature usually doesn't come by itself. Often there is also a certificate identifying the signatory and one or more time stamps marking certain events. Such certificates and time stamps are no more than small digitally signed files. This fact acerbates the problems of preserving digital signatures.

E-Signatures in court

One might expect that the law remains indifferent to the way in which evidence is preserved, as long as its authenticity can be demonstrated to the courts. As a rule, this approach is followed in criminal cases and generally regarding the proof of all matters of fact. In these cases, any and all evidence is admissible regardless of its form.[14] The records preserved by Alice, Bob and Carl can all be presented in court, leaving it to the judge to make up his own mind whether these records are convincing.

In many jurisdictions, limits apply to the admissibility of evidence where legal transactions are concerned. The reasoning being that the parties generally plan these transactions beforehand and are in a position to document the process in a reliable fashion. The parties are not allowed to burden the courts with shaky evidence unless they have a good excuse.

In Belgium, a signed document – in original form – must be presented for all private agreements exceeding the value 375 €.[15] 'Original form' means the document that features the parties' original signatures. In the case of paper documents, it means the piece(s) of paper that was (were) in the hands of the parties and signed by them.[16] In

---

[12]O. LIBON and S. VAN DEN EYNDE, *European Electronic Signature Standardization Initiative—Trusted Archival Services,* European Commission 2000, pp. 22-23 available on <http://www.law.kuleuven.ac.be/icri>.

[13]See J.-.F. BLANCHETTE, *La conservation de la signature électronique: perspectives archivistiques,* o.c., p. 24 ff.; O. LIBON and S. VAN DEN EYNDE, *o.c.*, pp. 17-32.

[14]Illegally obtained evidence is a notable exception to this principle and will not be discussed any further here.

[15]Art. 1341 Civil Code. See BOUDREZ, F., DEKEYSER, H. and DUMORTIER, J., *Digital Archiving: The new challenge?*, o.c., p. 16 ff.

[16]An 'original' in the legal sense is not necessarily unique. The Civil Code states that as many originals must be created as there are parties with a distinct interest in a contract (Article. 1325)

the case of digital documents, the meaning of the term 'original' is not as clear cut. Certain is that the digital file with digital signatures as appended by the parties qualifies as an 'original'. The advantage of presenting an original as evidence of an agreement is that it constitutes sufficient proof of the terms of the agreement on its own. Alice, Bob and Carl all start out with such original documents.

Carl does not preserve the digital originals, but replaces them with copies on paper. In principle these copies do not carry any weight in court. However, if the adversary does not demand that an original is produced, the judge may not request this of his own accord. The copy will be treated as if it were an original to prove the agreement. Even if the adversary protests the lack of proper evidence, all is not lost. Subject to certain conditions, any written piece of evidence may be presented. Of course, a document that you created yourself is not evidence, only documents originating from the adversary count. Moreover, to compensate for the lack of a signature, supporting evidence must be provided. So Carl must demonstrate that he has a paper copy of an electronic original emanating from his adversary and confirm its contents with additional evidence.

Alice discards all digital signatures and replaces them with metadata. As such, metadata containing authentication data can be considered a simple electronic signature. The judge may not disregard this signature just because it is in electronic form or is not a QES. Belgian law may very well reject this generic electronic signature because it is not the original signature as it was created by the signatory. Alice's documents will be treated as copies, just like Carl's. The fact that Alice re-signs the migrated documents has no bearing on their status as copies, neither does the involvement of a third party in the archiving process.

Bob makes every effort to preserve his signed documents in their original form. If successful, he can present proper documentary evidence to a judge and has fulfilled his burden of proof completely. Problems may arise if the digital signatures can no longer be validated due to bit degradation or incompleteness of the validation chain. Though the document loses its status of an original, it may still be regarded as a copy if all the conditions are met. The situation is worse if the record is no longer readable and no emulator is available. Little does it matter that the digital signature is valid if the underlying document is inaccessible. From a legal point of view, having a migrated version of the record as well, doesn't change the fact that the original is illegible. Bob can of course present the migrated record as evidence in its own right, though it too will be treated as a copy.

The insistence on preservation of 'originals' is not unique to Belgian Law. Other European countries have similar rules in place.[17] Nor is the predilection for originals limited to contractual law. An illustration of both these points is found in the Directive on Electronic Invoicing.[18]

In order to have a valid invoice, the authenticity of its origin and the integrity of its content must be guaranteed. These goals can be achieved through a multitude of archiving strategies. Member States may however demand that all invoices be

---

[17]France and Luxembourg have very similar rules of evidence requiring documentary evidence for private agreements (art. 1341 of the French and Luxembourgian Civil Code respectively). Germany mandates re-signing of QES's before the parameters and algorithms used become unsuitable when signed records must be preserved in original form (Section 17 Signaturverordnung).

[18]Directive 2001/115 amended Directive 77/388/EEC with a view to simplifying, modernizing and harmonizing the conditions laid down for invoicing with respect to value added tax, O.J., L 15/24.

preserved in their original form. Belgium is one of the countries that has used this option, thus barring Carl's hard copy strategy for invoices. Moreover, the Directive favors two techniques for the creation of valid invoices, namely the advanced electronic signature or an EDI format agreed upon by the parties. Only these two techniques must be accepted by Member States, others are optional. Bob's strategy of preserving original records complete with signatures fits neatly into this framework. Alice, however, may run into trouble. In Belgium, it seems that migrating invoices runs afoul of the obligation to preserve invoices in the form in which they were received.[19] Discarding the signature of an invoice authenticated by AES is not allowed either.

The examples given here show that the law's appreciation of various preservation strategies does not necessarily correspond with the criteria used by an archivist. This should be kept in mind when selecting a preservation strategy.

Transforming evidence

In the preceding sections we have seen that the law has a tendency to favour records preserved in original form rather than in other ways. The question is whether this preference is justified when it comes to digital records.

Copies are somewhat distrusted because the copying process can introduce errors and presents an opportunity for willful manipulation. In a past where copies were transcribed by hand, this was a very realistic assumption. Automated copying methods are less error-prone, but still present ample opportunity for foul play. In the legal context, originality of the record – and more importantly of the signature written on it – serves as a proxy for authenticity. Paper records are fairly easy to preserve, so the requirement to preserve originals is reasonable.[20]

The legal requirement to preserve originals is less suited to the digital environment. As it stands, the law tends to favor emulation as an archiving strategy, especially for signed records. From an archival point of view, there is no good reason to choose one preservation strategy to the exclusion of all others. The eDavid digital preservation strategy relies on a combination of emulation and migration.

Preserving fully functional digital signatures – complete with validation chain – and simultaneously maintaining readability of signed records is a complicated and therefore expensive operation. Migration or conversion of records is a reality of digital archiving. Sooner or later, the law will have to find a way to deal with such transformed pieces of evidence in an efficient way. Instead of clinging to originality, other clues about the authenticity of a record should be taken into account. The most obvious source of clues is the system in which the records reside. Of course, the reliability of a recordkeeping system depends heavily on the trustworthiness of its keeper.

A number of non-binding international legal texts encourage legislators to let go of

---

[19] See art. 60§3 par. 3 Belgian VAT Act. Possibly, the VAT Administration or the courts will adopt a liberal interpretation of this requirement, allowing migration at least to some extent.

[20] Even so, the costs involved in maintaining large paper archives has prompted legislators to allow transformation of evidence in certain circumstances. In Belgium, amongst others a number of public sector agencies and the financial, banking and insurance sectors were granted this privilege. France and Luxembourg have expanded the role of copies in civil evidence law under stringent conditions. (See the French law nr. 80-525 of July 12th 1980 and the Luxembourgian law of December 22nd, 1986).

the originality requirement.[21] The E-signature Directive takes a rather tentative step in the right direction with the definition of generic electronic signatures.[22] This shift is largely obscured, due to the emphasis on the AES and QES, which for all intents and purposes are the digital versions of an original handwritten signature. Likewise, the E-Invoicing Directive takes two steps forward and one step back.

Digital signatures are relied upon in the legal world to play the same role as handwritten signatures. However, both authentication methods function according to a different logic. These differences should be acknowledged in an appropriate way by the legal system. Looking at digital records from a long-term preservation perspective, the originality requirement appears to be inadequate. The legal framework needs to reserve an appropriate place for evidence that has undergone a transformation in order to be preserved.

Hannelore Dekeyser

ICRI – K.U.Leuven

[21] Recommendation (81) 20 of the Council of Europe and the UNCITRAL Model Law on Electronic Commerce.

[22] Any electronic data which serves as a method of authentication falls within its scope. Hence not only an original electronic signature may qualify, but also reliable metadata detailing validation results of defunct advanced or qualified signatures.