

Hannelore Dekeyser

Authenticity in Bits and Bytes

2006

<https://doi.org/10.25969/mediarep/13239>

Veröffentlichungsversion / published version
Sammelbandbeitrag / collection article

Empfohlene Zitierung / Suggested Citation:

Dekeyser, Hannelore: Authenticity in Bits and Bytes. In: Sonja Neef, José van Dijck, Eric Ketelaar (Hg.): *Sign Here! Handwriting in the Age of New Media*. Amsterdam: Amsterdam University Press 2006, S. 76–90. DOI: <https://doi.org/10.25969/mediarep/13239>.

Nutzungsbedingungen:

Dieser Text wird unter einer Creative Commons - Namensnennung - Nicht kommerziell 4.0 Lizenz zur Verfügung gestellt. Nähere Auskünfte zu dieser Lizenz finden Sie hier: <https://creativecommons.org/licenses/by-nc/4.0>

Terms of use:

This document is made available under a creative commons - Attribution - Non Commercial 4.0 License. For more information see: <https://creativecommons.org/licenses/by-nc/4.0>

Authenticity in

Bits and Bytes

Introduction

Writing has been instrumental in bringing mankind to where it is today, without it, accumulating the amount of knowledge currently at our disposal would have been unthinkable. Writing has also shaped the legal system into what we know today. The existence of nation-states with national laws, as opposed to local customary law, is to a large extent a legacy of the printing press, which allowed for legal texts to be spread fairly quickly over large regions.¹ In this legal landscape, handwriting has continuously served as the authentication method of choice.

The development of information technology is a revolution of at least the same magnitude as the printing press. We are only beginning to see its implications for society in general and the law in particular. In this paper, a very small aspect of this revolution will be explored, namely the issues involved in finding a substitute for the handwritten signature suitable for the information society. To narrow the subject down further, the focus will be placed solely on developments in western continental Europe, with Belgian law as a case study.

In the first section, a brief overview will be presented regarding the role played by handwriting in general and the signature in particular throughout history. Subsequently, two practical cases – the private contract and the last will and testament – will be discussed in order to demonstrate the role that handwriting still plays in the current legal system. In the following section, the transition to digital writing will be discussed, starting with an introduction to digital signature technology and continuing with a short exposition on the legislation enacted to pave the way for electronic signatures in the European Union. Finally, a comparison will be made between handwritten and digital signatures as legal authentication methods.

In this paper, I will argue that, although legislation was enacted to accommodate electronic signatures, ample evidence remains that the paradigm of handwriting has not yet been traded for a new one. From a short-term perspective, this does not appear to be problematic. However, in the long term a number of serious issues surface with regard to the durability of digital documents.

Brief Historic Introduction

Before diving into the turbulent waters of the digital age, a brief excursion into legal history is in order. Writing has not always enjoyed the privileged status that it currently has in the eyes of the law; in Roman and medieval times, for example, witness testimony was generally preferred, as it was possible to engage in cross-examination. From the 16th century onwards, documentary evidence gradually gained increasing legal standing. In western continental Europe, this evolution culminated in the evidence rules laid down by the Napoleonic codes, which firmly established the prevalence of documents over witness testimony (Macneil 2000, 7-9; Van Eecke 2004, 77). Documentary evidence became mandatory for certain transactions and was the only form of evidence admissible in court, with the express exclusion of witness testimony.²

The use of handwritten signatures as a method of authentication is also a relatively recent custom. Any use of documentary evidence – as such or in support of witness testimony – entailed the inclusion of a reference to the person bound by the document in question. Throughout history, seals, signets and handwritten marks were used for this purpose. In Roman and medieval times, seals and signets received more legal credit than handwritten marks (Van Eecke 2004, 86). As literacy increased towards the end of the Middle Ages, documentary evidence was more often drawn up by the parties themselves instead of dictated to a scribe. Gradually, the handwritten subscription which usually accompanied a seal or signet gained more legal weight as, unlike a seal or signet, only the signatory was capable of placing it.

This evolution was compounded by the introduction of surnames at the end of the 10th century. At the outset, the choice of a surname was more or less free, but by the 16th century it was customary to pass on a father's surname to all of his children (Van Eecke 2004, 104; Pintens 1981, 14). From that time, the handwritten signature, much as we know it today, all but replaced the use of seals and signets in western continental Europe (Van Quickenborne 1985; Van Eecke 2004, 87).

Handwriting in the Law

Two examples demonstrate the role that handwriting still plays in the current legal system: namely the private contract and the last will and testament. In terms of the Napoleonic tradition, a binding agreement is concluded when the parties agree on its contents (Article 1108, Belgian Civil Code). An oral agreement as such is valid and binding. However, a document signed by all parties involved must be drawn up for agreements exceeding a specified value. This document is sufficient evidence of the agreement and contradicting witness testimony is inadmissible in court (Article 1341, Belgian Civil Code). The reasons for this preference are pragmatic: the terms of an oral agreement are notoriously difficult to prove in court. The law goes one step further for some exceptional transactions by demanding that a document be drawn up as a requirement for the legal act to exist, in addition to proving its

terms. It is often the case that certain predefined handwritten notifications must be included in the document as well.³

Another legal act that calls for handwriting is the last will and testament. In Belgium, as in many other countries, a will can take the form of either a public instrument; a holographic will; or a so-called international will. In the first two cases, handwriting is an essential requirement for the validity of the will. To this date, a public will requires that the testator dictate his dispositions to the notary in the presence of two witnesses, or alternatively, two notaries (see Articles 971-975 of the Belgian Civil Code). The notary is obliged to record the will in person and by hand. Afterwards, the will must be read aloud before it is signed by all present. The presence of witnesses, by and of itself, is still sufficient evidence of the contents of the will. In the opinion of the Court of Cassation, it is irrelevant whether the witnesses are paying attention to what is being said, as long as they are in a position to verify whether all formal requirements were fulfilled.⁴

As the name implies, the holographic will is a document entirely handwritten by the testator (see Article 970 of the Belgian Civil Code). To be valid, it must be dated, signed, and it must mention where it was drawn up. Witnesses are not required and the will does not have to be registered to be valid.

The international will, by contrast, does not have to be written by hand.⁵ The will must be handed over to a notary in the presence of two witnesses, either openly or in sealed form. The testator must declare the piece to be his last will and must then sign it or formally recognize his signature if it is already present. Then, the notary must date and sign the will. Finally, the witnesses must place their signature at the bottom of the will. The notary must fill out and sign a form in duplicate, stating that all of the formalities have been fulfilled. The will is sealed in the presence of the testator and both witnesses and is then archived by the notary.

From these examples, it is apparent that the signature is the *prima donna* of evidence law. Until very recently, this term referred exclusively to handwritten signatures. A manually signed document is traditionally granted such high probative value in light of the properties that legal scholars attribute to it (see Dumortier, Van Eecke, and Anné 1999, 54-56; Gobert, and Etienne Montero 2004, 220-230). Firstly, the signature identifies its author in a unique way. Secondly, the signature expresses consent with the contents of the document. For this reason it has always been insisted upon that the signature is placed by hand directly upon the document itself, the use of carbon paper, seals or stamps is prohibited.⁶ According to some scholars, the signature protects the integrity of the document as it signals that the document is complete (see Dumortier, Van Eecke and Anné 1999, 52; Van Eecke 2004, 152; Van Quickenborne 1985, 5-6). Any additions below the signature or in the margins of the text are to be disregarded unless they, themselves, are signed. Each page of a long document is often signed separately to ensure pages are not inserted or replaced afterwards.

The high regard in which a signed document is held, is most obvious in the difference in status between an original and a copy. Only an original document is sufficient documentary evidence of agreements exceeding a certain value (see Article 1341 of the Belgian Civil Code; Verheyden-Jeanmart 1991, 201 ff). The essential

characteristic of an original document is precisely that the signature was placed directly upon it; any document derived from the original, but lacking an original signature, is merely a copy with less probative value. The method used to create the copy, for instance photocopying; use of carbon paper; or scanning is of no importance. The copy is admissible in court, but the adversary may demand the production of the original. However, if the copy is not challenged, the judge must presume it to be a faithful rendering of the original and treat it as such.

The Myth of Self-Authentication

In the hierarchy of evidence, the signed document is the highest form of proof. In view of the properties attributed to it in legal literature, the original signed document appears to be a self-authenticating form of proof. Upon closer examination, this picture becomes somewhat unraveled (Dumortier, Van Eecke, and Anné 1999, 54).

Where the identification function is concerned, handwriting in general, or a signature in particular, only serves as a reliable way to identify the author under the right conditions. When a signed document is presented as evidence in court, the presumed author is usually already known. Without any contextual data, identifying the author of a particular piece of handwriting is like searching for a needle in a haystack. In principle, the signature should consist of the signatory's last name, but this has been interpreted with some flexibility by the courts; the Court of Cassation emphasizes that the signature must be the handwritten mark that the signatory usually places in order to manifest himself towards others.⁷ In this spirit, even signatures that are illegible to the point that they give no clue whatsoever about the signatory's identity are often accepted. The bottom line is that verification by the court in the case at hand must be possible (see Van Quickenborne 1985, 22). Clearly, far from providing instant identification of its author, a signature generally requires the presence of contextual information to perform this function. The necessary context can consist of an acknowledgement by the signatory or the availability of reference signatures.

Even when it is known who the supposed author is, there is still the issue of forgery. So real is the risk of forgery that the law allows the presumed signatory of a contract to denounce 'his' signature as fake, and his heirs may suffice by saying they are not familiar with the testator's handwriting or signature – in either case, an expert witness must be appointed to determine whether the signature is genuine or not (Articles 1323-1324, Belgian Civil Code).

Concerning the second function, inducing consent merely from the presence of a signature is not self-evident either. Clearly, it is only by legal convention that the handwritten signature implies consent with the contents of a document, be it a contract or a will. Moreover, signatures are placed in other circumstances without implying consent, for instance, the witnesses present at the drafting of a public will do not express consent by signing, but only signal their presence at the occasion.

With regard to the third function – guaranteeing the integrity of documents – signatures are not the most efficient method to use. Primarily, it is not the signature, but the medium of paper, which guarantees the integrity of a document (see Gobert and Montero 2000, 23; Wilms 1995-1996, 839). Although not impossible, it is difficult to alter text on a page in an undetectable way. Documents that are entirely written by hand offer somewhat more protection against alterations by third parties, although they remain vulnerable to alterations made by the original author. The law takes these risks into account by making forgery a criminal offence. Also, to limit the risks in a contractual setting, the parties are required to create as many originals of bilateral agreements as there are parties with a distinct interest. Some very important transactions must be entrusted to a notary, who is responsible for guarding the integrity of his archives.

Even though in reality the handwritten signature does not live up to all its ascribed functions perfectly, these functions were still normative in the search for a substitute suitable for the information society.

A Signature for the Information Society

Paper is no longer the medium of choice to record, distribute, and receive information, as, to a large extent, information and communication technology (ICT) has taken its place. Evidently, as this technology is based on electronic pulses represented by zeros and ones, ICT does not accommodate handwriting very well. For legal systems that only recognize manual signatures, the writing was on the wall – an alternative had to be found to fulfill the functions of the signature, and, by extension, of handwriting.

A guiding principle in the adaptation of the law to the digital age is functional equivalence theory, a model first used by the UN Commission on International Trade Law (UNCITRAL) for the development of the Model Law on Electronic Commerce in 1996. This approach starts from an analysis of the purposes and functions underlying traditional paper-based requirements with a view to determining how those purposes or functions could be fulfilled electronically (see <<http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>>).

Bearing functional equivalence in mind, the legal world saw great potential in asymmetrical encryption technology as the ideal electronic substitute for the handwritten signature. This technique was promptly dubbed digital signature technology. Asymmetrical encryption certainly presents some useful properties for authentication purposes, although it is not without its limitations.

Digital Signature Technology in Brief

Digital signatures do not resemble handwritten signatures in any way. Where the handwritten signature is a graphical mark with a more or less stable form, the digital signature is unique for each file to which it is appended. The reason for this is

that the digital signature is derived from the file to which it belongs by means of a series of complicated mathematical computations.

In a first step, a hash value or so-called digital fingerprint is calculated for the file to be signed. Hashing is a technique by which electronic information can be reduced to a unique fixed-length code: if even a single character in the file is modified in transmission or storage, the resulting hash value will change. By comparing the original hash value with the current one, one can determine whether a document has been altered or not. Of course, the original digital fingerprint must be safeguarded against manipulation if it is to be compared later on with a newly calculated hash value. This is where encryption comes in. Encryption entails that a plain text message is transformed into a cipher text that seems meaningless. Symmetrical encryption means that the encryption key is only shared by the sender and receiver of the message. This protects against manipulation by third parties, but both sender and receiver could impersonate the other by using the common key. Asymmetrical encryption avoids this problem by giving each party his own pair of keys, one that must remain secret and another that may be made public. A text encrypted with one of the keys can only be decrypted with the corresponding key from the pair.

Asymmetrical encryption can serve two purposes. Alice can use Bob's public key to encrypt a message and send it on to him and, as only Bob has the corresponding private key at his disposal, no one else will be able to decrypt the message. Confidential messages can be sent safely through open networks this way. Conversely, Alice can encrypt a message with her private key and send it to Bob, who uses Alice's public key to decrypt it. As Alice's key is publicly available, anyone can decrypt this message. The point here is that Bob can be sure that Alice is the author of the message, as only she knows the corresponding private key.

There is one caveat to this story, however. Neither the hash value, nor the private or public key refers to Alice's identity in any way, as these are just numerical values. In this sense, the term digital seal would be more accurate for this technology. Bob must use other means to find out who the rightful owner is of the public key. Perhaps it was created by Carl, who is impersonating Alice. Alice and Bob could exchange public keys in a face-to-face meeting, but this is not always feasible. Also, Carl may have stolen the private key from Alice after this meeting took place. In open network environments, like the Internet, a public key infrastructure must be in place in order to tie public keys to the identity of their rightful owners.

A public key infrastructure offers a number of services related to digital signatures. Firstly the service of creating key pairs with which digital signatures can be placed. A second service is public key certification, whereby the link between a public key and its rightful owner is published for the benefit of recipients of signed documents. Depending on the type of certificate, the owner's identity is checked more or less thoroughly. Typically, a directory is kept of all certificates issued as well as a revocation list, which is important in the case of the theft of a private key. Lastly, time-stamping is an important service, as it is necessary to know whether a digital signature was placed before or after revocation of the public key certificate. To summarize, a digital signature is a small, encrypted file that is derived from the

file to be authenticated. To validate the signature, the signatory's public key must be used to decrypt the signature and information about the public key's rightful owner must be obtained.⁸

Digital Signatures and the Law

The properties of digital signatures as described above attracted great interest from the legal community around the world. A technology that allows one to identify the sender of a message, guarantee its integrity, and preclude repudiation by the sender after the fact is a prime substitute for handwritten signatures in the information society. In Europe, several legislative initiatives emerged to codify digital signatures.⁹ In order to ensure a harmonized legal framework for the internal market, the European Union issued Directive 1999/93/EC on electronic signatures.¹⁰

Initially, the idea was to enact rules attaching legal value to digital signature technology but this path was subsequently abandoned due to concerns about the longevity of a law tied to one type of technology. Therefore the legislators carefully avoided explicit references to digital signature technology in the wording of the directive. The term electronic signature is used and given a broad meaning in an attempt to create a technologically neutral legal framework.

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). A regular e-mail with the sender's name placed at the bottom can be considered an electronically signed document in this sense. The legal value attached to electronic signatures as such is fairly weak. Electronic signatures may not be discriminated against in court just because they are electronic (Article 5, §2 E-signature Directive), but they may be dismissed on other grounds.

A stricter definition is given for a subcategory of electronic signatures, namely the advanced electronic signature. The requirements are that the signature is uniquely linked to the signatory and is capable of identifying the signatory, that it is created using means under the sole control of the signatory and that it is linked to the relating data in such a manner that any subsequent change of the data is detectable (Article 2, 2° E-signature Directive). In the current state of technology, only digital signature technology can fulfill all these requirements.

Advanced electronic signatures, accompanied by a qualified certificate and created by a secure-signature-creation device, enjoy a special status in the directive. In legal literature this type of advanced electronic signature is usually termed a qualified electronic signature. Such qualified electronic signatures must be admissible as evidence in legal proceedings and must receive the same legal consequences as a handwritten signature would in similar circumstances (Article 5, §1 E-signature Directive). The benefit of the qualified electronic signature is that it has the same legal value in the whole internal market.

In transposing the E-signature Directive, the Belgian legislator literally copied the definitions of electronic signatures in general and qualified electronic signa-

tures in particular.¹¹ In contrast to the directive, the advanced electronic signature was given specific legal consequences as well.¹² For the purpose of creating original proof of a private agreement, the handwritten signature may be replaced by an electronic signature that can be attributed to its author and that guarantees the integrity of the document it is supposed to authenticate.

Functional Equivalence Theory in Practice

With regard to digital signature technology, two questions arise: How well do digital signatures perform the authentication functions expected of a signature and how do they compare with handwritten signatures?

Concerning the identification function, a digital signature alone does not reveal the signatory's identity, as it is just a computer code. Unlike a handwritten signature, a digital signature does not contain any direct reference to a person. However, depending on the contents and the reliability of the accompanying certificate, the signatory can be readily identified. Thus, both the handwritten and the digital signature require the presence of contextual information in order to be useful, albeit for different reasons.

The theft of a private key is problematic, as is forgery in the case of handwritten signatures. By law, the legal risks of this happening are distributed among the parties involved. The rightful owner is responsible for the use of his private key, until he revokes it (Article 19 §2 CSP Law). If the owner neglects to do so, the owner can be held liable for any damages under tort law. After revocation, any recipient of a signed document must consult the revocation list. Of course, the person unlawfully using the private key can be sued for damages by either party (Montero, 43-45).

When it comes to the expression of consent, it is but a social or legal convention that placing a signature entails consent to the signed document, as is the case for handwritten signatures. Digital signature technology makes this fact all the more evident, as machines are perfectly capable of digitally signing documents without any human intervention. Already, various automatic processes use digital signature technology for security reasons, with no intention whatsoever of expressing consent on anyone's behalf. Digital time stamps, for example, are nothing more than digitally signed text files containing the hash value of a file and an indication of the time of receipt.

With regard to the integrity function, digital signatures are touted as the perfect way of ensuring the integrity of signed documents. Although not false, this claim should not be taken at face value. Firstly, digital signature technology does not actively protect integrity, it only signals if the integrity of the bitstream has been compromised. Modifications in the bitstream may or may not entail a significant change in the contents of the signed message. If the money owed in a contract is changed from 100 to 1,000 per item, the integrity of the contractual terms is clearly compromised. If one pixel in a photograph changes from one shade of gray to another, this is probably not at all relevant for the message conveyed. Single bits

'falling over' is a common occurrence and rejecting any file where this has occurred would be overreacting. Digital signature technology is only capable of signaling integrity on the bit level, not on document level. This limitation makes it a rather fragile authentication tool.

Digital signatures make no pretense whatsoever of producing self-authenticating documents. This technology claims to be functionally equivalent to the handwritten signature, which does appear justified, at least if one only takes short-term perspectives into account.

Long-term Prospects for Signed Documents

The validity of documentary evidence, notably wills and contracts, usually only becomes an issue a long time after their creation. In comparing handwritten and electronic signatures, the durability of these authentication techniques must be investigated as well.

On average, manually signed paper documents are easy to preserve, even for extended periods of time. Under the right conditions, paper records can be kept for hundreds of years. Several copies of the Gutenberg Bible, printed in 1455, still exist today (see <http://en.wikipedia.org/wiki/Gutenberg_Bible>).

By contrast, the shelf life of digitally signed documents is dubious. As hinted above, the greatest strength of digital signature technology, signaling manipulation of the bitstream, is also its greatest weakness. Validation of a digital signature is only possible as long as the original bitstream remains perfectly intact. The perfect storage of bitstreams, even for a relatively short time, remains a challenge in itself. Even storage media that are specifically designed for this purpose, like CD-WORM disks, suffer from bit degradation to the extent that all readers come equipped with software to correct errors (see Boudrez, 10; Starret 2000). Digital signature technology by itself does nothing to prevent any changes to a bitstream.

Storing computer files intact is only part of the story. In itself, a bitstream is of little interest to us as it is not readable by humans. Both the necessary hardware and software must be available to translate the bitstream into an intelligible format on screen or in print. Hardware and software platforms come and go at an alarmingly high rate, resulting in the obsolescence of the file formats that depend on them. An example of what this can lead to is the case of the CNES (Centre National des Etudes Spatiales, France), which was forced to have documents that were created in 1985, re-typed manually in 1990 and again in 1997, because the newer generations of word processors could not read the original files with sufficient accuracy (Valoris 2003, 38). In order to cope with file format obsolescence, archivists generally put forward two distinct strategies, namely migration and emulation.

Migration entails the translation of a computer file into a suitable archival format. Depending on the specifics of the format chosen, the characteristics of the original file may be preserved or lost. For instance, when converting MS Word files to flat file, 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 document is preserved, but the ability to reuse the content is lost instead. Distinguishing between essential and incidental characteristics is the responsibility of the archivist. Whichever format is chosen, migration breaks any digital signatures accompanying the original file, as the new file is represented by its own distinct bitstream.

With regard to the preservation of digital signatures, emulation appears to be a more promising archival strategy. The functions and behavior of the obsolete platform – meaning the old hardware, software or both – is recreated on a contemporary computer platform, allowing the original files to be accessed. Notwithstanding some exceptions, current emulators are still in a highly experimental phase of development.¹³ Developing emulators is very difficult, especially for platforms that are not fully documented, and as a consequence, the costs involved are considerable. It is highly unlikely that emulators will be created for all possible platforms that exist today and for all future platforms to come. Moreover, emulators developed to run on today's platform will become obsolete in their turn, making either a chain of emulators or constant redevelopment necessary. If this chain is broken or redevelopment is omitted, the original file is lost, as it can no longer be accessed (Boudrez 2005, 83-84). The fact that the digital signature accompanying the file can still be validated offers little consolation.

Even if abstraction is made of these hurdles, the digital signature itself is at risk of becoming obsolete. Asymmetrical encryption works on the assumption that it is practically infeasible to crack the code by trying all the possible key combinations because the necessary computer power is not available. As time goes by, however, ever more powerful computers are developed, and eventually trying all the key combinations becomes a distinct possibility. Alternatively, flaws may be found in the encryption or hash algorithm, opening up new avenues of attack (Libon and Van den Eynde 2000, 22-23). To alleviate these problems, the length of the encryption keys is increased to match the pace of computer development and new encryption algorithms are introduced. Of course, this does not offer a solution for the legacy of digital signatures. Once the key or the algorithm is broken, fake digital signatures, indistinguishable from genuine ones, can be created.

One proposed solution to the weakening of digital signatures, is re-signing old signatures with more recent technology (see Blanchette 2004, 24 ff.; Libon, and Van den Eynde 2000, 17-32). Although certainly technically feasible, this scenario quickly becomes very cumbersome. Not only the obsolescence of the digital signature itself must be taken into account, but also of the certificate identifying its rightful owner and any available time stamps. Such certificates and time stamps are no more than small files digitally signed by the service provider.

Archivists feel that the investment in time and effort to preserve fully functional digital signatures is just not worth it. Instead of applying costly procedures to ensure the integrity of the signature and the entire validation chain behind it, they propose to invest only in ensuring the integrity of the document itself. In this scenario, any signatures accompanying a document will be transformed into metadata, which mention who authenticated the document at a certain point in time (Blanchette 2004, 32-36 ff.).

From a long-term perspective, digital signatures perform poorly in comparison with handwritten signatures. This does not imply that digital signature technology should be abandoned, only that appropriate measures should be taken to counter such shortcomings. Several technical and organizational possibilities are proposed by archivists and engineers, but the question remains to what extent these are accommodated by the legal framework.

Leaving Originality for Authenticity

The legal community still lives with assumptions and expectations rooted in the paper environment. One of these is the idea that the original signature must be preserved. For paper documents, this is a reasonable requirement, as a handwritten signature on a paper medium is relatively easy to preserve, even for extended periods of time. Moreover, the signature continues to fulfill its authenticating functions more or less identically throughout its life span. Thus an original document provides the same clues to determine its authenticity on the day of its creation as it does 50 years later.

Originality is a good proxy for authenticity with regards to paper documents, but this is not the case for digital records. As digital signatures are difficult to preserve and lose their authenticating functions after a relatively short period of time, indications about the authenticity of digital records should be sought elsewhere. The most obvious source of clues about document authenticity is the system in which these documents reside. Of course, the reliability of a record-keeping system is a function of the trustworthiness of its keeper.

By way of example, the e-invoicing Directive takes a clear step away from requiring originality in favor of a more direct evaluation of authenticity.⁷⁴ Electronic invoices are valid as long as the ‘authenticity of their origin and the integrity of their content’ remain guaranteed. However, member states may impose invoices to be preserved in the form they were sent, either on paper or electronically and thus may choose to uphold the originality requirement to some extent, but they are not encouraged to do so.

In the e-signature Directive, the originality requirement is still present in both concepts of advanced and qualified electronic signatures. By definition their creation must be under the sole control of the signatory and the signatures themselves must guarantee the integrity of the document they accompany (see Art. 2 §2d Electronic Signature Directive). Qualified electronic signatures enjoy a privileged legal status, but their preservation along with the entire validation chain is cumbersome.

A very tentative step away from the originality requirement can be found in the generic definition of electronic signatures as given in the E-signature Directive. 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. However, the legal status of generic electronic signatures is somewhat vague

and undefined. The member states need only ensure their admissibility before the courts on a non-discriminatory basis; this means that an electronic signature may not be rejected just because it is electronic, though it may be denied legal value because the technology used is unreliable. Still, this concept opens the door for the courts to evaluate the authenticity of the documents presented to them directly by assessing the reliability of record-keeping systems and the trustworthiness of their keepers.

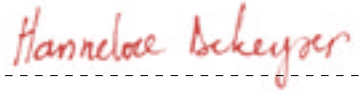
In Belgian law, the admissibility of generic electronic signatures has been introduced as mandated, though the advanced electronic signature has taken precedence in the areas of law where it matters most, for instance, regarding the law on evidence of contractual obligations. The revised Civil Code starts off by broadly stating that an electronic signature must be attributable to its author, but then it goes on to say that the signature itself must guarantee document integrity. In other words, the originality requirement still shines through. There are some preexisting exceptions to the originality requirement that may provide a backdoor for a more direct approach to examining document authenticity. However, this only provides a solution for a limited number of cases.

As it stands, the law favors emulation as an archiving strategy. In practice, there are other factors to be taken into account, specifically cost-effectiveness and risk. In the end, it comes down to the parties involved to decide what costs they are willing to incur in order to preserve their digitally signed documents. Some will opt to preserve their digital signatures complete with validation chain, in order to benefit from their privileged legal status. Others may decide to entrust their signed records to a third party custodian, vouching for authenticity on the basis of the reliability of his record-keeping system. As standard best practices with regard to the preservation of digitally signed documents evolve, the inappropriateness of the originality requirement for digital documents will become increasingly apparent.

Conclusion

The rise of the information society has forced legal scholars to look at basic concepts from an entirely different angle. One result of this exercise has been the enactment of legislation paving the way for electronic signatures. Upon closer inspection, ample evidence exists that legislators have yet to trade the paradigm of handwriting for a new one. The legal value of the qualified electronic signature is explicitly linked to that of handwritten signatures, which marks it as a transitional concept. The definition of the advanced electronic signature mimics the workings of handwritten signatures. As a consequence, this type of signature is rigidly bound to its original form, making signed documents highly vulnerable to technological obsolescence. The generic electronic signature does not suffer from these constraints, but the legal certainty it provides is low. Basically, citizens can either strive to fulfill the originality requirement for their digitally signed documents or venture into uncharted territory.

Although electronic signatures are called upon in the legal world to play the same role as handwritten signatures, both authentication methods function according to a different logic. Looking at the long-term perspective for signed documents makes this very clear. Instead of trying to force one into the mould of the other, these differences should be acknowledged in an appropriate way by the legal system. For one, the appropriateness of the originality requirement should be assessed in this light. More generally, a legal frame of reference should be developed for the evaluation of authenticity and authentication of digital documents.



Hannelore Scheyer

SIGN HERE!

Notes

1. The influence of the media used for communication on law is the subject of Katsch, Ethan, *The Electronic Media and the Transformation of Law*, 347. New York: Oxford University Press, 1989.
2. Articles 1320 and 1341 of the French Civil Code of March 21, 1804. Subject to various modifications, this Civil Code is still in force in France and Belgium.
3. Two examples are the unilateral promissory note pertaining to a sum of money (Art. 1325, Belgian Civil Code) and the consumer credit agreement (Art. 14 of the law of June 12, 1991 on Consumer Credit, *M.B.* July 9, 1991), which must both contain certain handwritten notifications in order to be valid.
4. Belgian Court of Cassation, May 4, 1979, Pas., 1979, I, p. 1047-1048, excerpt available on <<http://www.cass.be>>.
5. The convention providing a Uniform Law on the Form of an International Will (Washington, DC, October 26, 1973) was introduced into Belgian law by the law of January 11, 1983 (*Moniteur Belge*, October 11, 1983).
6. See Belgian Court of Cassation, June 28, 1982, Pas., 1982, I, p. 1286-1292. and Van Quickenborne, M., 1985, p. 23 ff.
7. A holographic will inscribed simply with 'mother' was denied any legal value, although there was no discussion about the testator's identity, see Belgian Court of Cassation. January 7, 1955, Pas., 1955, I, p. 456 and Van Quickenborne, M., 'Quelques réflexions sur la signature des actes sous'. In *Révue C.J.B.*, 10, 1985.
8. For a more detailed description of digital signature technology, see Dumortier, J., P. Van Eecke, and I. Anné, *The Legal Aspects of Digital Signatures*, II, I.c., Gent: Mys and Breesch 1999, 21-48.
9. The German Bundestag passed the Multimedia Law (Gesetz zur Regelung der Rahmensbedingungen für Informations- und Kommunikationsdienste, July 22, 1997, *Bundesgesetzblatt*, I, 1997, p. 1870) and Italy passed law no. 59 of March 15, 1997 to allow the use of electronic documents for legal transactions. Around the same period, other European nations were preparing similar legislation, see Dumortier, J., P. Van Eecke, and I. Anné, *The Legal Aspects of Digital Signatures*, IV, Gent: Mys and Breesch 1999, 125.
10. See 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>>.
11. 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).
12. See Art. 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).
13. Emulators have been successfully developed for various game consoles, but also for other computer systems, see <http://en.wikipedia.org/wiki/List_of_emulators>.
14. 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.

Works Cited

- Belgian Civil Code, Articles 970, 971-975, 1108, 1341 and 1325.
- Belgian Court of Cassation, January 7, 1955, Pas. 1955, I, p. 456; May 4, 1979, Pas., 1979, I, pp. 1047-1048, excerpt available at: <<http://www.cass.be>>; and June 28, 1982, Pas., 1982, I, 1286-1292.
- Blanchette, J.-F. *La conservation de la signature électronique: perspectives archivistiques*. Paris: La Documentation Française, 2004.
- Boudrez, F. 'Electronic Record Keeping', in: Boudrez F., H. Dekeyser, and J. Dumortier, *Digital Archiving: The New Challenge?* Louvain-la-Neuve: I.R.I.S., 2005.

- Boudrez, Filip. *CD's voor het Archief*. Stadsarchief Antwerpen, Antwerp and Leuven: ICRI K.U. Leuven, p. 10, available at: <<http://www.antwerpen.be/david>>. Directive 1999/93/EC of the European Parliament and of the Council of December 13, 1999, *Official Journal*, January 19, 2000, L13/12, Articles 2, 1°; 2, 2°; 2 §2 d; 5, §1 and 5, §2, available at: <<http://www.europa.eu.int/eur-lex/nl/index.html>>.
- Dumortier, J., P. Van Eecke, P., and I. Anné. *The Legal Aspects of Digital Signatures*. II, Gent: Mys and Breesch, 54-56, 1999, available at: <<http://www.law.kuleuven.ac.be/icri/>>.
- French Civil Code, March 21, 1804, Articles 1320 and 1341.
- Gobert, Didier and Etienne Montero. 'La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle', in *DA/OR* 2000. <http://en.wikipedia.org/wiki/Gutenberg_Bible>. <http://en.wikipedia.org/wiki/List_of_emulators>. <<http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>>.
- Katsch, Ethan. *The Electronic Media and the Transformation of Law*. New York: Oxford University Press, 1989.
- Libon, O., and S. van den Eynde. *European Electronic Signature Standardization Initiative – Trusted Archival Services*. European Commission 2000, available on <<http://www.law.kuleuven.ac.be/icri>>.
- Macneil, Heather. *Trusting Records Legal, Historical, and Diplomatic Perspectives*. Dordrecht: Kluwer Academic Publishers, 2000.
- Montero, Etienne. 'Définition et effets juridiques de la signature électronique en droit belge: appréciation critique', in: Montero, Etienne (ed.), *La preuve*. Formation permanente, 54, Liège: ULg. Formation Permanente CUP.
- Multimedia Law (Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste), German Bundestag, July 22nd, 1997, *Bundesgesetzblatt*, I, 1997.
- Pintens, Walter. *Naam*. In: *APR*, Story-Scientia, Gent, 1981.
- Starret, Bob. 'Compact Disc Errors', in: *Roxio CD-R Newsletter*, April 21, 2000, available at: <<http://roxio.com/en/support/cdr/cderrors.html>>.
- Uniform Law on the Form of an International Will (Washington, DC, October 26, 1973), Intro. to Belgian law by the law of January 11, 1983, *Moniteur Belge*, October 11, 1983.
- Valoris, *Comparative Assessment of Open Document Formats Market Overview*. Report for the European Commission, DG Enterprise, 2003.
- Van Eecke, Patrick. *De handtekening in het recht, Van pennentrek tot elektronische handtekening*. Brussel: Larcier, 2004.
- Van Quickenborne, M. 'Quelques réflexions sur la signature des actes sous', in: *Révue CJ B*. 1985.
- Verheyden-Jeanmart, Nicole. *Droit de la preuve*. Brussel: Larcier 1991.
- Wilms, Wilfried. 'Van handtekening naar elektronische notaris - de validering van elektronische communicatie', in: *R. W.*, 1995-1996.