8

On Long-Term Storage of Digitally Signed Documents

Jon Ølnes[1] *, Annikken Bonnevie Seip **
* *PKI Consulting Services AS, P.O.Box 1569 Vika, N-0118 Oslo, Norway*
** *Statskonsult, P.O.Box 8115 Dep, N-0032 Oslo, Norway*

Abstract: The term "digital signature" is a metaphor that seeks to describe a particular use of public key cryptography by use of the well-known "signature" term. The political direction in most parts of the world is towards wide acceptance of electronic documents, and introduction of electronic signatures to replace handwritten ones. Where security requirements of any importance exist, digital signature is the only open electronic signature mechanism. This paper examines one particular aspect of digital signature usage, long-term storage. Technical difficulties and directions towards solutions are described, and sources of requirements (legal and other) are discussed. The conclusion is that storage cannot be regarded as reliable for more than about 10 years. This may cause problems in particular to e-government but is probably sufficient in most cases.

Keywords: Digital signature, legal aspects, archival, long-term storage, PKI.

1. INTRODUCTION

"Digital signature" is a metaphor that illustrates a particular use of public key cryptography by referral to the well-known concept of a signature. As most metaphors, this one has its pros and cons. The parallel to a hand-written signature serves the purpose of removing much of the "mystic" from the technology, but on the other hand it obscures the fundamental differences between a handwritten and a digital signature.

The politics in most parts of the world are geared towards widespread acceptance of electronic communication. In paper-based communication, signatures fulfil important functions, which are reflected in laws and

[1] Also part-time associate professor at the University of Tromsø, Norway.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35617-4_48
J. L. Monteiro et al. (eds.), *Towards the Knowledge Society*

regulations. Thus, legal compliance and the (at least medium-term) need to relate electronic communication to accepted procedures for paper-based communication create legal requirements for electronic signatures.

From a user viewpoint, requirements for electronic signatures are related to establishment of a sufficient level of security for communication, and sufficiently trustworthy procedures for electronic documents. One may argue that signatures are less important for electronic than for paper-based communication, since (transaction and other) logs may ensure the necessary traceability of the communication.

The term "electronic signature" is technology neutral, and notably used by the EU directive on electronic signatures (Directive 1999/93/EC, 1999) . "Digital signature" on the other hand refers to a particular technology for electronic signatures. If we apply the criterion that only the signer shall be able to produce a signature, then digital signature is the only open electronic signature mechanism.

When archiving a digitally signed document, one has two options:

1. Store the document with signatures intact, and ensure access to enough information to validate the signatures later if needed.
2. Store the document without signatures along with tracing of the signature validation process performed before archival.

Long-term archival of digital signatures (alternative 1) creates problems related to the limited lifetime of data formats, reconstruction of state with respect to expired keys and certificates, security over time of cryptographic algorithms and keys, and in general to the complexity of the technology. Some problems are more or less easily solved but our conclusion is that storage for more than 10 years cannot be regarded as reliable. But 10 years may be enough in most cases.

On the other hand, the second alternative may not yield sufficient trust and evidential value in all cases. In particular, this is related to the correctness of format conversions for documents where every footnote and figure must be preserved. An intact digital signature shows that conversion has not taken place. One must also trust the security of the archive against modifications.

Following a few introductory remarks in 2, 3 and 4, we describe the problems related to long-term storage of digital signatures in 5, examine alternatives in 6, look at the requirements for signatures and long-term storage in 7, discuss use as evidence in 8, and conclude the paper in 9.

2. A REMARK ON AUTHENTICATION AND TRUST

Questions have been raised (Clarke, 2001, Ellison et al, 2000) about the viability of digital signatures and the supporting technology, the PKI. After

all, public key cryptography has been around for more than 20 years, and we still have not really seen the breakthrough. One problem is that PKI services are marketed as "trust services". But a PKI provides authentication, not trust. Assurance of the identity of your counterpart is usually not sufficient to establish trust in the counterpart. Other trusted services, like brokers, are necessary to mediate trust between unknown parties. A digital signature (or other PKI-based authentication) is useful to the extent that the receiver can make use of the name in the certificate and relate this to other information about the signer, in order to evaluate if the trust is sufficiently high for the particular purpose.

The authors' view is that an infrastructure for authentication is highly useful, and that PKI is the most scalable and suitable technology for the purpose. Infrastructures are almost by nature complicated, and deployment takes time. With a deployed infrastructure, digital signatures will greatly facilitate such tasks as interaction between the private and public sector, banking, and health services (see 7).

3. THE PURPOSES OF SIGNATURES

A vital question to ask is: why do we sign? There is not a single answer to this. Answers will differ dependent on culture, practice, and the legal system in various countries. One suggestion for the purposes of a signature (Galtung et al, 1994) is:

- Identification function, by creating a link between the document and the name of the signer (authentication);
- Authorisation (and data integrity) function; the signature implies that the signer accepts the contents of the document or gives it a certain authority;
- Evidence function, where a signed document provides a stronger proof than a document without a signature (non-repudiation);
- Symbolic function, e.g. signing as a part of some ceremony;
- Fulfilment function, e.g. denoting the end of a negotiation process.

It is fairly clear that a digital signature can fulfil all these purposes, though people need to get more used to the technology, e.g. before the symbolic function is accepted. In the context of this paper, the question is to what extent digital signatures must be archived in order to fulfil the purposes over time. A further question is if, and under which conditions, electronic communication without signatures can fulfil such purposes.

It has been suggested, in particular by ETSI (ETSI, 2002), to use formalised signature policies that define the context and purpose of a digital signature in e.g. an electronic commerce transaction. Which role or authoritative power does the signer take by producing the signature? Such

initiatives link well to standardisation efforts in electronic commerce, such as ebXML[2] but we do not yet know if the idea will take effect.

4. ELECTRONIC AND PAPER DOCUMENTS

A signed paper document is a fascinating technology. Most information is gathered in the paper. The number of actants[3] is reasonable: the signer, the document, the signature, the receiver, and laws and regulations. We may want to divide the document actant into document contents, paper and ink. These three parts are concerned with the format of the physical document.

An electronic document has other and more actants connected to it: the format, editing program, basic software, hardware, and storage media. It need not necessarily be a limited (closed) amount of data, and multimedia technologies add flavours to the document term. With a digital signature, one must add signature format and cryptographic algorithms and keys with software or hardware implementation. For validation, there is access to public keys, network components, and online access to certificate information or whatever you want to check now or in the future. There will also be a need for competence to operate the validation process.

Two properties need to be in place in order to obtain a digital signature: the document must be a finite (closed) set, since one needs to compute a fixed hash value over the contents; and the document needs to be static since the hash must be re-computable in order to validate the signature.

WYSIWYS (What You See Is What You Sign) is a property that is desired for digital signatures. This means that the signer's view on the screen[4] is a complete and correct view of the document. Given that an electronic document may contain such features as hidden text and revision traces, and that the view of a document may depend on different local configurations for sender and receiver, the WYSIWYS property is not evident for most documents. On the other hand, a paper document is definitely WYSIWYS.

We see that a digital signature is fundamentally different from a handwritten signature, although the technologies may be used for the same purposes. Another major difference is that paper documents are based on a stable technology (paper and ink), while electronic documents and signatures depend on the quickly evolving and changing technologies used.

[2] Electronic Business using XML – http://www.ebxml.org – is a promising initiative in the electronic commerce area. The initiative is sponsored by UN/CEFACT and OASIS.

[3] Physical or logical artefact that constitutes a separate part of a certain process or interaction.

[4] Here ignoring other presentation media for multimedia documents.

5. LONG-TERM STORAGE, THE PROBLEM AREAS

A science-fiction short-story, that the authors no longer remember the name of, describes a future archaeologist in despair over trying to bridge the gap of about 50 years lack of written material from the period 2005-2055. It seems like all written documents from this period have vanished due to the electronic storage media or the document formats no longer being readable. This may be overly pessimistic but we do face problems. Long-term storage of a digitally signed document in particular has five problem areas:

- Lifetime of the storage medium;
- Lifetime of the keys and certificates used;
- Lifetime of the signing method, related to key sizes and other aspects of the cryptographic algorithms;
- Lifetime of the document, signature, and certificate formats;
- Lifetime and service offer of (trusted and other) actors involved.

As we shall see in the following, most of these are solvable, but document and signature formats pose severe problems. All aspects are difficult to handle for individual persons. The discussions below are partly based on (Seip, 1999) .

5.1 Lifetime for Storage Media

All storage media in use today – disk, tape, CD-ROM and others – are vulnerable, and will over the years become unreadable. One also has to consider technological progress, which renders old media obsolete. It is not easy today to find equipment that can read an old-fashioned magnetic tape.

These problems may be solved by routinely copying all archived material to new media. One should ensure that the material exists in more than one copy, preferably using different media technologies for the copies. The processes must render exact copies of the documents, to avoid undesired changes to documents and invalidation of signatures. The logistics related to such copying may be rather complex and time-consuming but it is quite evident that this will be practically possible.

5.2 Lifetime of Certificates and Keys

A person's handwritten signature is fairly consistent over time, and may be validated by a check against an authorised signature sample. One always signs in person, and other attributes related to the signature, such as role, must be deduced from the document.

Opposed to this, every digital signature is unique, and must be validated by means of public keys and certificates with limited lifetimes. The signature

binds to the name in the certificate, which will usually be the name of a person but may be a pseudonym, role or organisational name. The name may contain more attributes than just the name, e.g. an organisational affiliation. A name may be valid for only a short period, however if the certificate is valid, the name should be valid as well. As long as keys and certificates are valid, this poses few problems. After expiry or revocation, validation is harder.

The first observation is that the time-stamp for the signature must be reliable, in order to know exactly the point in time where certificates and keys must have been valid. Trusted time stamp services will be available (Adams et al, 2001), and should be used in cases where the actors' own time stamps cannot be relied upon. A time stamp consists of a signature covering the time and the hash value of the document, meaning in the simplest case only that the document existed at that time. To add more semantics to this, the time stamping must be included in the protocol for the communication between the parties, e.g. an electronic commerce protocol.

Following validation of the time stamp, one must then reconstruct the state at the given time with respect to certificates and revocation information. This information may be stored locally, or one may rely upon the certificate issuer (or some other trusted service provider). Relying on the issuer also means that one relies on the existence of the issuer – a clear risk since certificate issuers may go out of business. When validating a certificate, one must also ensure that the public key of the certificate issuer was valid at the given time.

For revocation checking, one may want to check the first CRL issued after the signature creation instead of the one valid at signing time[5], to capture revocations done during this CRL-issuing interval. Issuers that only use OCSP (Myers et al, 1999) or other on-line revocation checking must also provide a (on-line) service that can answer questions about an old certificate's validity at a given time. CRLs may be a better mechanism for revocation checking for expired certificates, as CRLs may be stored locally if necessary.

The section below discusses protection of old and weak signatures (key lengths no longer sufficient for protection) by countersignatures. If this is applied, a further validation step is of course added to the process.

5.3 Lifetime for the Signing Method

Recommendations for key sizes for public key algorithms are based on estimates of the processing power necessary to succeed in a brute-force

[5] Actually, this goes for real-time signature checking also but timing considerations usually prevents such delayed (wait for next CRL) signature validation.

attack on the key pair. There must be a sufficient number of possible key pairs to render such an attack infeasible even to a very powerful attacker.

For sustained protection, recommendations for key sizes must cater for technological development that continuously gives the attacker more and more processing power. A problem is that one may predict, although with uncertainty, the development of today's technology but it is impossible to predict the "quantum leaps" that occasionally occur in technology. E.g. what will the situation be like if major breakthroughs are made in areas such as quantum processing or bioinformatics? The corollary is that one cannot state anything really definite about the strength of a signature on a time scale of more than about 10 years.

Public key cryptography relies on mathematical theory that is not necessarily proven to be correct, like, for RSA, the one-way property related to numbers that are composed from large prime number factors. There is a risk that development in mathematics in the worst case will undermine a public key algorithm, or, perhaps more realistic, will provide more efficient methods for attacking the one-way function that is the foundation of the algorithm in question. This may lead to a requirement for larger key sizes.

Additional weaknesses may be related to the implementation of the cryptographic algorithms, one example being insufficient quality of the key generation process. Such weaknesses, detected in retrospect, may severely weaken signatures created using the implementation in question.

Prolongation of the lifetime of a signature may be achieved by protecting the old and weak signature by a new, sufficiently strong countersignature that covers the document and previous signatures. The countersignature must be trusted to at least the same level as the original signature, and it must be clear that the producer of the countersignature has not firstly exploited the weakness in order to alter the document and produce a faked, old signature.

We will not go into details with respect to protocols for such protection of old signatures, but only refer to Nilsson and Pinkas (Nilsson et al, 1999) who show that this is possible but also that it is potentially very complicated. Nilsson and Pinkas discuss a situation with very limited trust between the actors, and thus high security requirements, and their suggested system may be considerably simplified if the requirements are less severe, and in particular if trust between the actors is higher.

5.4 Lifetime of Formats and Technology

A digital signature binds to the document format that was signed. Format conversion invalidates a signature. Electronic document formats have a limited lifetime. As one example, the Norwegian computer manufacturer Norsk Data had a fairly high penetration in the Norwegian market until they went out of business around 1990. Documents written in their document

editing system, NOTIS, are now hardly accessible, as very few working Norsk Data computers remain.

This experience is not particular to the NOTIS case, not even the event of a company vanishing from the market. A parallel question today may be: What is a Word document worth in 10-15 years? Some software manufacturers are willing to maintain backward compatibility or at least some support for old versions for a rather long period of time but it is difficult to predict the market situation 10 years or more ahead, and whether these manufacturers still survive or change strategies.

This calls for document formats with an expected longer lifetime. Such formats exist, with SGML, XML (which is a subset of SGML) and EDIFACT (suitable only for well-defined messages) as the most common examples. Standards that are deployed and used[6] will usually have a fairly long lifetime. Robustness is added through support in products from different vendors. However, even SGML and XML must be expected to have a limited lifetime, and a prediction ranging more than 10-15 years ahead is highly risky. Besides, the signer must be able to handle SGML if this shall be used as archive format for the digitally signed documents. This may be a tall order.

Signatures are added to a document according to a signature format specification. Again, storage with digital signatures intact must be done in the format delivered by the signer, and both the document format and the signature format must have a sufficient lifetime. Following the EU directive (Directive 1999/93/EC, 1999), ETSI works on specifications of signature formats (ETSI, 2001). Specifications for signing of XML have quite recently been finished (Eastlake et al, 2001). Specifications for signing of EDIFACT exist as well but the mainstream recommendation here is to wrap the message (or interchange) in the general PKCS#7 format (Kaliski, 1998) .

The ETSI specifications and the XML specifications are not yet deployed. They must be tried in real life before their lifetime can be predicted. However, PKCS#7 (or CMS (Housley, 1999), which is derived from PKCS#7) may be used to sign (and encrypt) almost anything, provided the content exists in a single file. This provides at least one standardised signature format that is stable and deployed.

The last information elements that must survive over time are certificates and CRLs. Today, these are almost exclusively defined by the X.509 standard (ITU-T, 1997), although some alternative certificate formats exist. X.509 in turn relies on the ASN.1 syntax for specifications. Given the XML digital signature specifications (Eastlake et al, 2001), it is clear that even certificates may be defined in XML. There is no work on XML certificates at present as far as we know, and the approach has its disadvantages as well,

[6] ODA – ISO standard for Open Document Architecture – serves as an example of a document standard that never left the paper.

e.g. a much larger footprint must be expected than for the ASN.1 alternative. However, a prediction that XML certificates will prevail in perhaps 5 years may not be unrealistic, leaving the faith of old X.509 (and ASN.1) certificates in a 10-year perspective rather uncertain. Old certificates can probably be converted to a new format and signed again with the same information content "in retrospect", but this picture is not entirely clear, and requires a trusted service that takes care of the conversion.

5.5 Lifetime of Trusted Actors

Any processing that relies on the continued existence and operation of some external actor carries a risk. With respect to long-term storage, leaving archival of old certificates and revocation information to the certificate issuer will cause problems if the issuer later goes out of business or alters its service offer. Relying on specialised validation service providers carries the same risks. However, the alternative is to maintain all information needed in-house, which creates a severe logistics problem. The risk of relying on manufacturers has already been exemplified by the Norsk Data case.

5.6 Problems for Individuals

Document management is a hassle, even to large organisations, not to mention individuals. People may have reasonable control of their paper documents but less control over their electronic documents across generations of home-PCs or similar equipment. The risks of accidental destruction are evident, and eventually important documents, with digital signatures, will only be available in electronic form. One cannot print a digital signature. In addition to document management, programs needed to read old documents and to validate their signatures must be installed on new equipment.

Individual users cannot be assumed to handle validation of old signatures on their own even if they may over time learn to manage their electronic document archives. The solution may be services that offer "electronic vaults", where users may deposit electronic documents that they need to archive. A service should be run in a way that makes it sufficiently trusted as a third-party witness (notary) with respect to a document as genuine and integrity protected. Requirements for storage of digital signatures (or validation traces only) with documents depend on the service offering. If the user may change documents, and no securely stored copy of the original version or adequate change log exists, then signatures may be needed.

5.7 Summary

All the aspects discussed in this section must be tackled properly in order to safely validate an old digital signature. In a perspective of up to perhaps 10 years, this should be possible in a reliable way, but our conclusion is that one cannot today expect digital signatures to be reliably archived for more than these 10 years – perhaps a bit less if one wants to add a safety margin. However, 10 years may be more than enough in most cases, and even 10 year old handwritten signatures may have a questionable value.

Maintenance of document archives with digital signatures is today only possible for organisations with reasonable competence and a well-organised IT-infrastructure. All other actors, and in particular individuals, will need assistance, either from certificate issuers, or from other service providers. The main problem in long-term storage is document formats that either must be preserved together with programs and equipment necessary for their processing, or be subject to format conversions that today still cannot be expected to yield 100% correct results.

6. ALTERNATIVES TO SIGNED ARCHIVAL

Two alternatives exist related to archival of signed documents:

- Do not use digital signatures at all but rely on other means to achieve the necessary traceability (non-repudiation) of the communication;
- Remove signatures and store only a trace of the validation process.

Most legacy systems will maintain communication logs and transaction logs that record events such as the arrival of an electronic message (document) with exact time and identification of source, and transactions that resulted from the message. If these logs are well protected, and the source was authenticated as a part of the communication procedures, then this may constitute sufficient linking between the "signer" (the authenticated source) and the document. This depends on the trust between the actors, and possibly on the role of neutral, trusted parties. However, the discussions in 7 show that even if one can do without digital signatures in many cases where a paper signature would be needed, there are other cases where in particular legal requirements demand use of digital signatures. Thus, the first alternative does not cover all cases.

Although the conclusion is that digital signatures are needed, the need to archive them is not that evident. As one example, the Norwegian archive law and its regulations (NOARK-4, 1999) state that a digital signature may be removed from a document before archival, provided that evidence of the signature verification process is recorded. The main reason is that the document may have to be converted into one of the approved storage

formats, and this conversion will anyway invalidate signatures. Effectively, this means writing, in the document or to a separate log, text stating that this document was signed by the named parties, that the signatures were supported by identified certificates from named certificate issuers, that the certificates were neither expired nor revoked, and the name of the person or system that performed this process. The log entry, or the changed version of the document, should have a trustworthy time-stamp, and may be digitally signed by the archive system or the person responsible for the process. Following this process, one no longer has a signed document, but a witness statement that the document was signed.

For this to be acceptable, one is dependent on the security of the whole process and on secure storage of the document after removal of signatures. The main contribution of a digital signature from a security perspective is protection against manipulation by the intended recipient of a document. Thus, if signatures are removed before archival, the procedures must protect against such manipulation to a similar degree. This may call for archival at some neutral, trusted party instead of in-house.

7. REQUIREMENTS FOR DIGITAL SIGNATURES

7.1 Legal Requirements

In all legislations, one will find laws and regulations that have explicit requirements for signatures. To cater for electronic communications in such cases, "electronic signature" (Directive 1999/93/EC, 1999) has been coined as a technology-independent term that shall cover all existing or future means for signing an electronic document. This term is used in political and legal documents in order to keep the technology independence.

"Digital signature" on the other hand is a term that means use of public key cryptography to obtain an electronic signature. If the requirement is that only the signer shall be able to perform the signature creation process, then digital signature at present is the only open method for electronic signatures[7]. If this requirement is relaxed, other means may be used. Some definitions of the electronic signature term (van Eecke, 2001) include passwords / PIN-codes and other authentication mechanisms as a kind of signature. A particular interpretation (regulation) of a law may then accept use of a PIN-code as a "signature". This will typically only be acceptable when security

[7] There are some products based on pen and pen pad with sensors to record biometrics related to hand-written signatures, with cryptographic binding to the document. These systems must be regarded as closed and proprietary See for example PenOp: http://www.penop.com

requirements are rather lax. For electronic signing of documents with more severe security requirements, digital signatures will be required. Examples may be areas such as taxation (and other) reporting to public authorities and the health care sector.

Most legislative work on electronic signatures specifies them as a replacement for handwritten signatures. Usually, the first steps towards use of electronic documents relate the use to accepted procedures. The electronic procedures more or less mimic the paper-based communication. This may be necessary in order to gain acceptance for electronic communication in the short term, but it is too restrictive in a more long-term perspective. It is generally accepted among experts that a transition from paper-based to electronic communication should be accompanied by an analysis of work procedures and such, in order to gain full effect from the transition. Such analysis should also investigate the use of and need for signatures.

Another reason to devise electronic signatures as replacements for paper-based signatures is the fact that, when a law states a requirement for signatures, it is easier to change the (interpretation of) the law to encompass electronic signatures than to perform a thorough evaluation of whether signatures are at all necessary for electronic communication for the particular purpose, and in case under which circumstances.

7.2 User Requirements

From a user perspective, a digital signature's main contribution is the non-repudiation function, which is protection against modification (not against deletion) by the correct receiver of a document. If the receiver is not sufficiently trusted, the sender may want to insist on using a digital signature. The receiver may also require a signature in order to obtain stronger evidence, and avoid the risk of being accused of manipulation. In other words, user requirements for signatures arise when the trust between the actors (mutual or one-way) is too low for communication and transaction logs to be sufficient.

With respect to long-term storage of signatures, in particular the trust in the actors' logging and archival procedures is important. A procedure that removes signatures and only stores traces of the validation process will only be acceptable if either the actor has a sufficient level of trust (a bank or some public service may be examples), or archival is done by some external party. If the actor's archival procedures are not trusted or unknown, one must take particular precautions with respect to own archival of signatures. Note that one is always in a position to fake ones own signatures, unless countersignature or other protective means, e.g. related to time stamp services, are used.

7.3 Requirements for Long-Term Storage

Archival and storage of documents – electronic or paper-based – may be at the discretion of the involved parties or in some cases mandated by laws and regulations. For the public sector in Norway, some types of documents shall be archived by the organisation handling the case for at least 25 years. Indefinite archiving is required for documents that are deposited at the National Archives of Norway.

Following the political direction of equivalence between paper based and electronic communication, in principle this calls for indefinite archival of electronic documents and digital signatures. We concluded in 5.7 that archival of digital signatures for more than 10 years must be regarded as unreliable. Thus, even the 25-year timeframe above is unrealistic[8].

We noted in 6 that the Norwegian archive law and its regulations (NOARK-4, 1999) under certain conditions allow removal of a digital signature from a document before archival. The full legal implications of such removal are not resolved in Norway or in any other country as far as we know. The process described, if securely performed and with adequate security for storage of documents and logs, will probably in many cases yield sufficient evidential value.

Iit must be pointed out that the process of removing signatures and converting documents is critical and not sufficiently described at present. For example, the Norwegian archive law and regulations (NOARK-4, 1999) have no requirements for the security and quality of the process described (signature validation, document conversion, storage of signature validation traces – possibly with a signature from the archiving person or system). It is evident that this process must have a security and quality level that at least matches the original signature. Security requirements are particularly imposed on the storage of signature validation traces, and on secondary signatures by archiving systems/persons. The quality requirements imposed on a document conversion tool that must yield 100% correct results, even for documents where every footnote and figure is of vital importance, are probably in general impossible to meet today.

Given the complexity and security requirements of the process, this should be delegated to specialised long-term storage services, which may also take the role of a notary service. We already see storage services offered both as outsourcing services related to internal IT-services, and as open services on the Internet. The latter is particularly viable to individuals, who may need electronic deposit boxes or personal archives for their documents (that are very difficult to manage across generations of home-PCs). Given a

[8] 25 years storage of electronic documents (without digital signatures) and related logs is also complicated but may be achievable. Evidence backed by 25 years old log entries may be questionable but the court value of (signed) paper documents also diminishes over time.

sufficient (high!) quality and security level, and a neutral actor in charge of the service, a storage service should, from a security point of view, be able to remove digital signatures from the stored material in most cases without any seriously deterred security to the involved actors. The lawmakers, and not the technologists, should probably decide on the necessity of storage of signatures as far as legal requirements apply. However, there are ample examples of documents and processes where the requirements for signatures and their storage are at the sole discretion of the communicating parties.

Perhaps the best strategy to adopt is to archive documents with digital signatures as long as the document format can be easily processed, and remove signatures when document conversion is deemed necessary.

8. USE AS EVIDENCE

A (signed) paper document is a very tangible proof that is easily understood by any member of a court. On the other hand, an electronic document with digital signatures must be regarded as a complex proof with respect to the court members' judgements. A court may need to rely on a witness statement from some trusted party (or even from the actors themselves) about the validity of a digital signature. The court cannot in the short term be expected to be able to validate old signatures itself (see 5.2). As far as we know, there is no court practice in any country with respect to challenging the validity of a digital signature, or basing a case on (primarily) a digitally signed document. The first actor that tries such a case faces an unclear juridical situation. One crucial question related to long-term storage is if validation traces will be sufficient to convince a court, or if signatures need to be archived, to be validated at the time of the trial.

An example of a similar case is a person that is defaulting on a loan, where the contract (IOU) for the loan is a digitally signed document. In many cases, a legal recovery of the debt need not go through a court but a warrant from some public official may be needed. In this case, the public official must either be able to validate the proof (the signed contract) itself or it must accept a witness statement about the validity of the contract. When such a simplified procedure is possible with paper evidence, the procedure with electronic evidence should be no more complex. A "qualified signature" as defined by the EU (Directive 1999/93/EC, 1999) shall in principle always give this intended effect. However, requirements for "secure signature creation environments" are not yet settled. It is questionable if one can produce such a signature on a standard PC.

9. CONCLUSION

Long-term storage of digitally signed documents cannot be relied upon for more than about 10 years. However, 10 years may be enough for most practical purposes. Problems are in particular related to formats (for documents, signatures, and certificates). A digital signature binds to the formats, which must be preserved together with equipment and software necessary for processing in order to validate old signatures. Other problems concern lifetimes of storage media, signature keys and supporting certificates, signing method (algorithms and key sizes), and continued existence of trusted actors that one relies upon for signature validation.

An alternative to archival of digitally signed documents is archival of documents without signatures, but with recorded traces of the signature validation process performed at document reception. With adequate security and quality of this process, and sufficient security of the archives, this may yield sufficient non-repudiation and evidential value. A neutral, trusted notary service should probably be used.

Perhaps the best strategy is to archive documents with digital signatures as long as the document and signature formats are easily readable. When this is no longer the case, signatures may be removed with validation traces recorded, and the document may be converted to a more modern format. The document will then probably already be at least a few years old. Note however that document conversion may also be an unreliable process today, especially if every footnote and figure must be preserved.

10. REFERENCES

Adams C., Cain P., Pinkas D., Zuccherato R. Internet X.509 Public Key Infrastructure Time-Stamp Protocol. RFC3161; August 2001.

Clarke R. The Fundamental Inadequacies of Conventional Public Key Infrastructure. Proceedings of the European Conference on Information Systems; June 2001; Bled.

Eastlake D., Reagle J., Solo D. XML-Signature Syntax and Processing. RFC3075; March 2001.

van Eecke P. European Legislation on Electronic Signatures, One Year after the Directive. ISSE Conference; September 2001; London.

Ellison C., Schneier B. Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure. Computer Security Journal; v. 16 no. 1 pp 1-7; 2000.

ETSI. Electronic Signature Formats. ETSI Technical Standard TS 101 733; January 2002. (Technically equivalent to RFC3126 Electronic Signature Formats for Long Term Electronic Signatures, September 2001.)

ETSI. Signature Policies Report. ETSI Technical Report TR 102 041; February 2002.

EU. Community Framework for Electronic Signatures. Directive 1999/93/EC of the European Parliament and of the Council; December 1999.

Galtung A., Riisnæs R. Court Aspects of Digital Signatures (in Norwegian). Institute of Computers and Law; Faculty of Law; University of Oslo; March 1994.

Housley R. Cryptographic Message Syntax. RFC2630, June 1999.

ITU-T | ISO. OSI – The Directory: Authentication Framework. ITU-T X.509 | ISO/IEC 9594-8; 1997.

Kaliski B. PKCS#7: Cryptographic Message Syntax Version 1.5. RFC2315; March 1998.

Myers M., Ankney R., Malpani A., Galperin S., Adams C. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. RFC2560; June 1999.

National Archives of Norway. NOARK-4, Norwegian Archive System Version 4. Part 1: Functional Description and Requirements Specification (in Norwegian). Kommuneforlaget; ISBN 82-446-0628-2; 1999.

Nilsson H., Pinkas D. Validation of Electronic Signatures. ID2 White Paper; January 1999.

Seip A. Long-term Storage of Digitally Signed Documents (in Norwegian). NR Report 948; Norwegian Computing Centre (NR); ISBN 82-539-0451-7; November 1999.