Digital signatures, timestamping and the corresponding infrastructure

Ahto Buldas, Helger Lipmaa

January 6, 1998

Abstract

One of the main factors for developing a well functioning legal background for the use of electronic documents as evidence in the court is the presence of a reliable timestamping infrastructure. Many countries are currently working on their national digital signature law. The current paper emphasises some of the problems arised during the work of the committee formed by Estonian State Chancellery to prepare the legal use of electronic documents, mainly concentrating on the work of the research group formed for the developement of timestamping techniques suitable for legal use.

1 Introduction

Because of the increasing importance of the international business and communication, it became necessary to forward signed documents to a long distance. Traditional mail system is too slow for the information society needs.

Radio, TV, Fax and Computer Networks made it possible to send information from one point to another with the greatest possible speed – the speed of light. Of course, the received electronic document cannot be viewed as original because:

- electronic documents can be easily copied and modified without detection;

- unlike hand-written characters, digitally encoded characters have not the individuality;
- the signature of an electronic document is not physically connected to the content of the document.

Due to these disadvantages electronic documents are not often considered to have any legal force.

Digital signature is a cryptographic technique that enables to protect digital information (represented as a bit-stream) from undesirable modification. It is widely used to protect data in secure e-mail systems. Digital signature can effectively substitute the hand-written signature in the electronic environment. In many countries the laws and regulations have been adopted which equalise the use and functions of digital signature to hand-written signature. However, non of these countries have any experience of using digitally signed data as an evidence in the court.

The legal use of electronic records is increasingly important. One of the reasons, as it has been said above, is that electronic documents enable to communicate much faster. Another reason is that the archives are full of old paper documents which have a legal importance but are used very rarely. Saving the space in archives is urgently needed. This helps to understand why the initiative to form the corresponding committee in Estonia became from the archivists. It became clear that the most important step towards the legal use of electronic documents is to enable the legal regulation of digital signatures. Before issuing a law on digital signature, clear understanding of the technical details necessary to support the law is inevitable. Thereby, the intensive cooperation of lawyers, archivists and data security specialists is needed.

Security techniques used in electronic documents have been developed keeping an eye on secure messaging systems. However, the secure maintenance of electronic documents with a long lifetime is a bit more complicated task. Numerous problems in this area have not been solved yet. Some of these have been regarded below from the viewpoint of data security specialists.

2 Meaning of the signed data

By ISO/IEC 2382-1 (1993-11-15) **information** is a knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning. Digital information is an information represented in digital form i.e. as a bit-stream.

In a paper document the representation of the information (text and pictures) is physically connected with the carrier (paper). Unfortunately, there are lot of different ways (**formats**) how to represent text and pictures as a bit-stream. Therefore, a bit-stream itself has no *a priori* interpretation.

Digital signature of a person is simply a function which assigns to a given bit-stream X another bit-stream X – the signature of X. Therefore, it is not clear from the signature which particular meaning of the bit-stream X has been taken into consideration. Of course, the owner of the signature cannot deny the fact that he has signed a bit-stream X, but nobody can prove the original meaning of X.

One solution to that problem is adding the format description into the signature. A format F is a function which assigns to a bit-stream X its meaning, i.e. a text, a picture etc. If there is an agreement that each format F has a unique code $n(F)$, this code can be included into the signature, i.e. the signature of X is $D(X, n(F))$. Unfortunately, there exist neither widely accepted agreements nor standards for that purpose.

However, such a solution has been planned to use in Estonia. Format encoding is viewed as an additional function of the Certification Authority (CA). If it is necessary to use a new format, it has to be registrated in the CA beforehand. A technical description of the format has to be available on-line and it has to be signed and timestamped by the CA. It is necessary, that different formats have different codes.

3 Private keys

Another problem related to the use of digital signatures is the management of the private signature keys. If somebody else, except the owner, gains access to the private key, he/she will be able to forge the owner's signatures on electronic documents. At that point even the value of legitimately signed documents can be called into question. Moreover, if the signer of a particularly important document (a loan agreement etc.) later wishes to repudiate his/her signature, he/she can dishonestly report the compromise of his/her private key.

Therefore, the verifier of a digitally signed document should be able to ascertain **when** the document was actually signed. Digital **timestamping** is a solution to this problem.

4 Hash functions

The computation of the one-way function D, used as a digital signature, is time-consuming. Thereby, using a hash function h to transform a bit-stream X to the bit-stream $h(X)$ of fixed length is inevitable. The real signature of X is therefore $D(h(X))$. The bad thing here is that the used hash function h may not be secure eternally (MD4). If there is an effective way to find other data X' such that $h(X') = h(X)$, the signature of X is not reliable. There are hash functions that are secure, provided that certain combinatorial problems are hard to solve. For example, the Chaum-van Heijst-Pfitzmann Hash Function is secure if and only if the discrete logarithm cannot be computed efficiently. Unfortunately, this hash function is not fast enough to be of practical use.

5 Timestamping

Most of the technical realisations of timestamping system use trusted third party called **TimeStamping Service** (TSS) [2]. The timestamp is a digital attestation of the TSS that an identified electronic document, subscribed with a digital signature, has been presented to TSS at a certain time. Timestamping system allows the verifier to determine reliably whether the digitally signed document was created during the operational period stated in the public key certificate.

If Alice wants to timestamp the signature $D_A(X)$ of a document X,

- she sends $D_A(X)$ to TSS.
- TSS adds the current time t to the signature, signs it with his private key D_{TSS} and sends $s = D_{TSS}(t, D_A(X))$ to Alice.

The last message s is called a **timestamp** of $D_A(X)$. If the signature and timestamp are added to the document X, one can reliably verify the signature even if the private key D_A is compromised. However, such a simple timestamping system has two serious disadvantages:

- TSS should be unconditionally trusted, i.e. it is impossible to verify whether the timestamp s was created actually at time t.
- If the private key of TSS is compromised, all the timestamps created up to that time can be called into question.

6 Linking the timestamps

Above mentioned disadvantages show that a secure timestamping system cannot rely on keys, or any other secret information. In order to diminish the need of trust, TSS can link all timestamps together into a chain using a hash function H. In this case the timestamp for $y_n = D_A(X)$ is computed as follows:

$$s_n = D_{TSS}(n, t_n, y_n, \mathrm{ID}_A, L_n),$$

where n is the number of the current timestamp, t_n is the current time, $\mathrm{ID}_A = \mathrm{ID}_n$ is the identifier of Alice, L_n is the linking information computed as follows:

$$L_n = H(n, t_n, y_n, \mathrm{ID}_n, L_{n-1}).$$

If the used hash function H is collision-free, the security of the timestamp system does not rely so much on the private key of TSS.

If Bob wants to verify Alice's timestamp which has been created a long time ago, he can sequentially verify all the timestamps between the Alice's timestamp and a timestamp which is trusted by him moving backwards along the chain of timestamps. Unfortunately, such a time consuming procedure is not useful in real systems. However, there is a better solution for linking timestamps together as presented in [1]. If each timestamp is linked not only with the previous one but also with another suitably chosen timestamp, the length of the verifying chain can be reduced to $O(\log^2 n)$, where n is the number of timestamps between Alice's timestamp and the timestamp trusted by Bob.

7 Renewing old timestamps

As it was told above, hash functions are not eternally secure. Unfortunately, this is also true for the hash function H used to link timestamps. Breaking of the hash function H means that all timestamps created up to that time are not reliable any more. Thereby, the periodical changing of the hash function is inevitable. Of course, the periodical change of H alone is not sufficient. Before the old hash function gets insecure, one should renew the old timestmps which still have a legal importance. The renewing of a timestamp can be initiated by each person interested in a further possible legal use of the corresponding document. Renewing procedure means simply that TSS creates a timestamp to an old timestamp [1].

8 Infrastructure

Single timestamping server may not be able to handle all the timestamping requests sent by its clients. Therefore, the timestamping job should be shared by several servers which can be organised hierarchically as Certification Authorities. Moreover, CA-s can themselves offer timestamping services, which means that an additional infrastructure is not needed.

In order to enable the verifying of timestamps of each other two timestamping servers may periodically link their timestamp chains together, by requesting timestamps for another server to their own timestamps.

Each timestamp server may have an individual security policy in which the following items should be present:

- Restrictions to the life-time of the timestamped documents.
- The authentication protocol.
- Frequency of changing the hash function.
- The signature scheme.
- Frequency of linking the timestamp chain with other servers.

References

[1] Buldas,A., Laud,P., Lipmaa,H., Villemson,J., "Ajatempli protokollid, turvavajadused ja tehnilised nõuded," Technical report, Cybernetica, 1997.

[2] Massias,H., Quisquater,J.-J., "Time and cryptography," Technical report, Université catholique de Louvain, March 1997. TIMESEC Technical Report WP1.