

Time Stamping of Environmental Information

Miroslav Hrad, Jiří Hřebíček, Jaroslav Ráček

Masaryk University
Brno, Czech Republic

Overview

- What is a digital time-stamp
- Time-stamp schemes
- Principles of time-stamping
- Conclusions

Trustworthy information

Exist many situations in crisis management when we need information to make a decision. And we ask:

Is this information trustworthy?

And also exist many situations after an accident when we ask:

Did anybody have information about the danger before this accident?

Who is a guilty of this accident?

To answer previous questions we need to know who and when important information was published.

Who and when?

Consider two questions that may be asked by a computer user as he or she views information in form of digital document.

- Who is the author of this document?
 - Digital signature
- When was this document created?
 - Digital time stamp (TS)

Which information should be time-stamped?

Could be useful to add time-stamps (digital signatures) to:

- data from monitoring
- information about decisions
- crisis plans
- ...

Nobody can change or manipulate information in future.

Digital Time Stamp

The digital time stamp is a technique to prove the existence of certain digital data prior to a specific point in time.

What is needed is a method of time-stamping digital documents with the following two properties:

1. Must find a way to time-stamp the data itself, without any reliance on the characteristics of the medium on which the data appears, so that it is impossible to change even one bit of the document without the change appearing.
2. It should be impossible to stamp a document with a different time from the actual one.

Time Stamping Schemes

Basic schemes of TS:

- **Simple scheme** (naive solution)
 - one TSA and no data included in other TS
- **Linking scheme**
 - data from another TS
- **Distributed scheme**
 - cooperation of more than one TSA

TSA - Time Stamp Authority (issuer)

Simple Scheme

Scenario:

- An entity that wants a time stamp for certain data D (requester) transmits a request message including a hash value H of D to an entity issuing a time stamp (issuer).
- The issuer (TSA) generates a digital signature S on data that includes at least H , a time parameter T and an identifier ID of the authority (TSA). T indicates the point in time at which the issuer received the request message. A time stamp TS corresponding to D includes at least H , T , ID and S .
- The issuer sends TS to the requester.

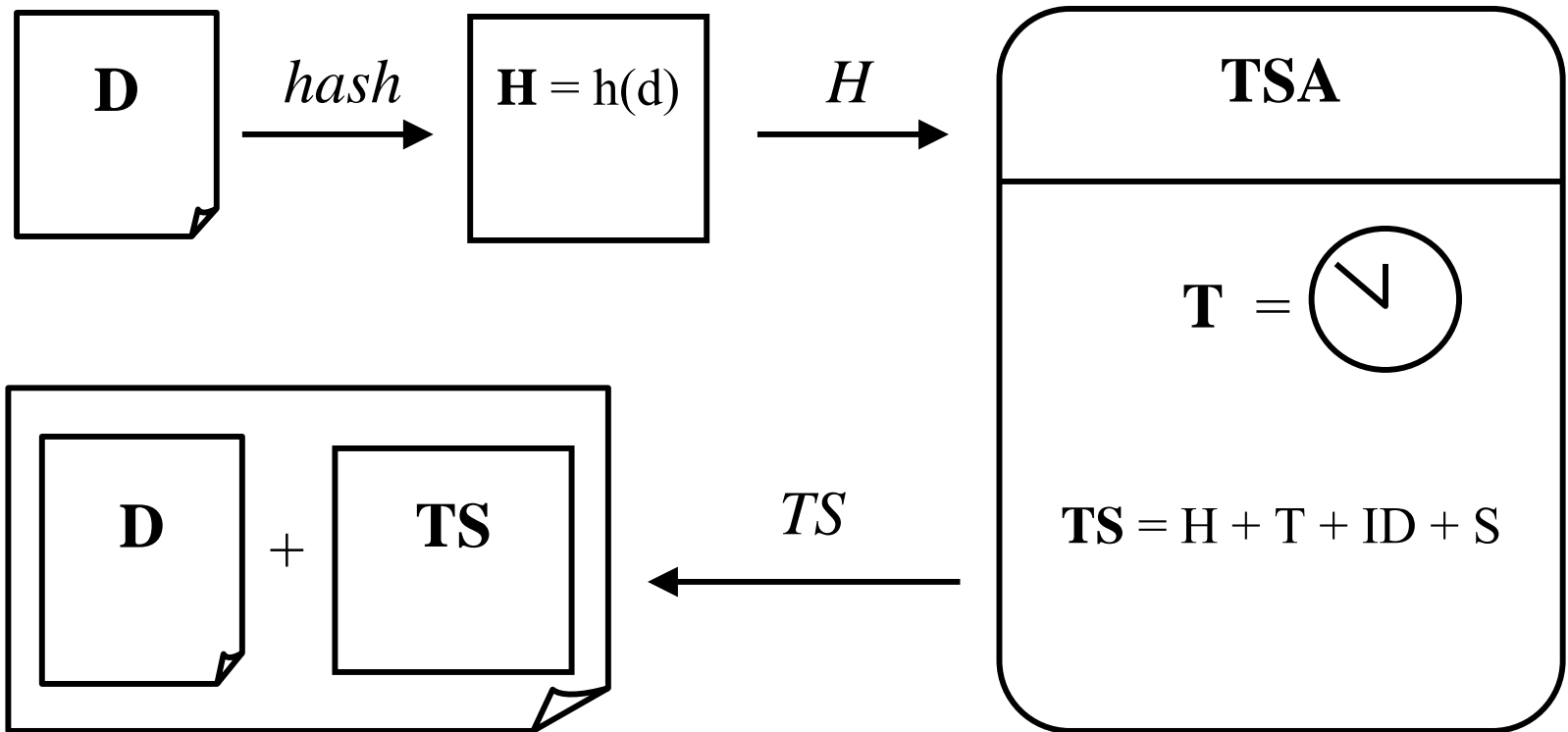
Hash Functions

Only hash value of data (document) can be time-stamped.
There is no need to send original data to TSA.

On the side of client (requester) is usually used some of one-way hash function:

- MD5 (Message Digest, 128 bits value)
- SHA-1 (Secure Hash Algorithm, 160 bits value)
- SHA-256 (Secure Hash Algorithm, 256 bits value)

Simple Scheme



Verification of TS

1. The verifier computes a hash value of D and compares it with H included in TS.
2. The verifier carries out an algorithm to verify S .

Verification of TS

The main characteristic of the simple scheme is that while its system is relatively simple, its security depends on time stamp issuer's reliability.

Nothing in this scheme prevents from colluding with a client in order to claim to have time-stamped a document for a date and time different from the actual one.

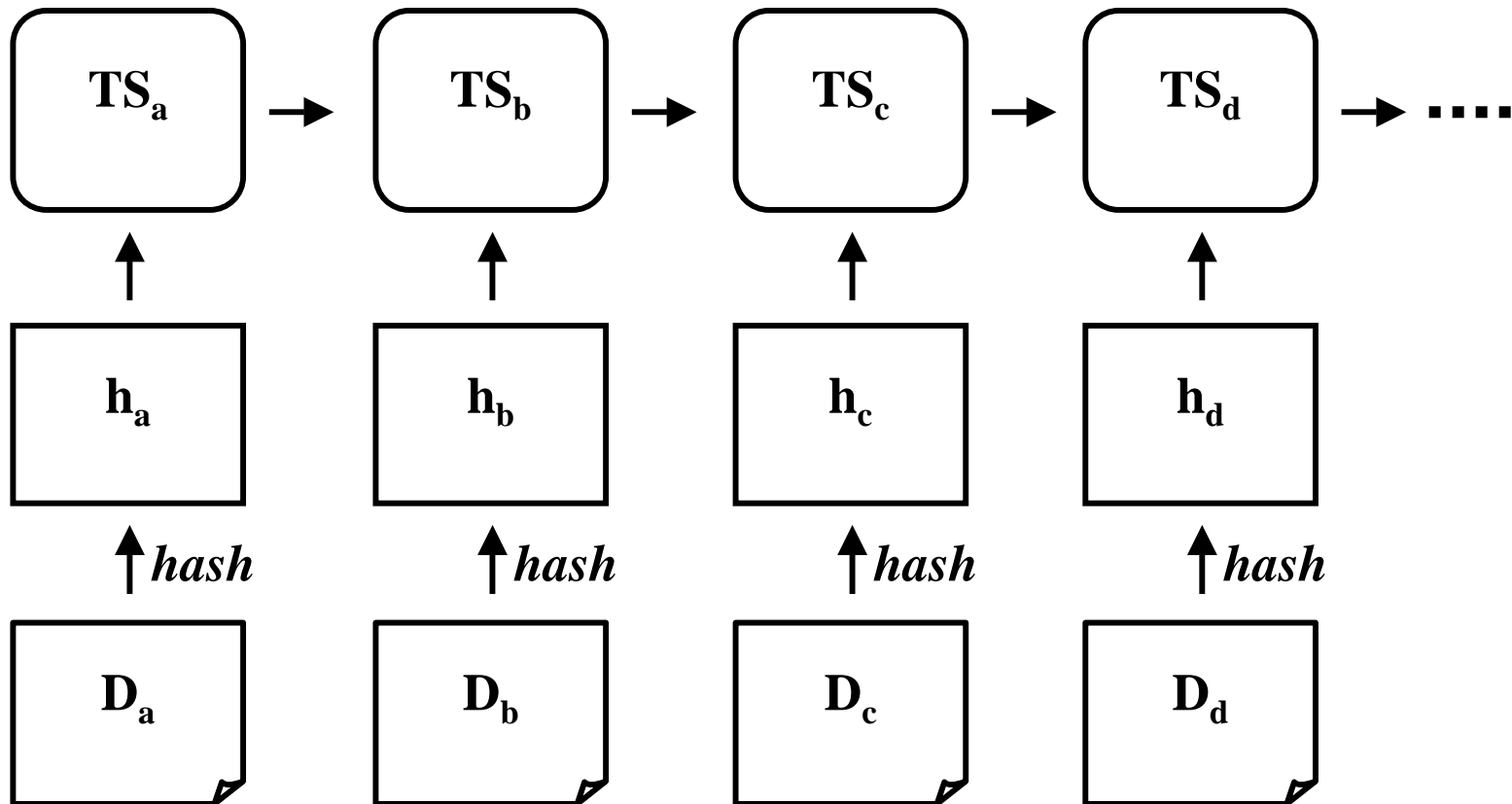
Linking Scheme

Issuer generates a time stamp which includes data included in other time stamps.

If an issuer is willing to fraudulently alter a certain time stamp, it has to alter all the time stamps relating to that time stamp.

It is considered to be more difficult for an issuer to manipulate a time stamp in the linking scheme.

Linking Scheme



Secure log

- variant of linking scheme
- a hash of previous TS is not included in the next TS
- exist the special reference record – secure log:

$$l_0, l_1, \dots, l_n, \dots$$

$$\text{where } l_n = h(x_n, l_{n-1})$$

TSA periodically (once per week) publishes last l_n from a secure log (web page, newspaper) and after that any TS included in secure log cannot be changed.

Distributed Scheme

The main aim of this scheme is to strengthen security against the issuer's manipulation of a time stamp by sharing the secret data used to generate a time stamp among the issuers.

The secret data are divided into n pieces in such a way that the secret data are easily reconstructable from any k pieces.

If the number of collusive issuers is less than a specific predetermined number, they cannot recover the secret data completely and therefore find it hard to manipulate a time stamp.

Signature after time t

How to demonstrate that data D was signed after time t and not before it?

- Requester A transmits a request to TSA.
- TSA generates a digital signature on actual time t and sends $H = \text{Sig}_{TSA}\{t\}$ back to the requester.
- Requester A adds trustworthy time information H to data D and generates digital signature.

$\sigma = \text{Sig}_A\{D, H\}$ is proof that data D was signed just after time t .

Signature before time t

How to demonstrate that data D was signed before time t and not after it?

- Requester A generates a digital signature on data D (creates $\sigma = \text{Sig}_A\{D\}$).
- Requester transmits σ or $h(\sigma)$ to TSA.
- TSA adds actual time t to σ and generates a digital signature on it.
- TSA sends $T = \text{Sig}_{TSA}\{\sigma, t\}$ back to the requester.

$T = \text{Sig}_{TSA}\{\sigma, t\}$ is proof that data D was signed just before time t .

Signature at an exact time

It is impossible to use time-stamp techniques to determine the exact time when the data was signed.

Usually it is proven that data was signed after time t_1 and before time t_2 .

Conclusion

It is a linking schema, which seems to be the best for using in crisis management today

- It is relatively fast and low-cost
- It is relatively trustworthy

Official TSA is not required in secure log based schemes.

Large area of usability (primary data, decisions, emitted documents etc.).

Thank you