Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Synchronizing Time Distribution

Sahar Adill Kadum[a]

[a]*Babylon University- Collage of Science for women, Babil, Iraq, Email: wsci.sahar.adil@uobabylon.edu.iq*

ARTICLE INFO

Article history:
Received: 13 /11/2022
Rrevised form: 20 /12/2022
Accepted : 26 /12/2022
Available online: 31 /12/2022

Keywords:

Time stamp
Distributed time stamp
Digital documents
Security
transaction

ABSTRACT

With the wide span of internet brought great progress in different parts of human life, a digital documents have been employed as a media in exchange information between internet parties like text, audio, pictures and videos that leads to the issue of how to certify the document when created or modified in order to use it as secure digital media for storing information and transactions. This tend to employ security technique for ensuring the documents integrity for a long period. One of these techniques is the time stamp that has many schemes. This research concentrate on distributed time-stamp scheme as a one of time stamp schemes, that suffers from drawback in achieving trusted security to overcome this draws a new technique issued to this scheme called "Synchronizing Process".

MSC..

https://doi.org/10.29304/jqcm.2022.14.4.1128

1. Introduction

The huge expansion in using internet has brought great progress in transactions between related parties that processed and recorded electronically as a digital documents. The documents have been used as a media for transferring, co-operation and storing instead of paper-based documents. However, the alteration in digital documents is difficult to detect rather than paper-based documents. Preserve document security over a long time period as paper-based documents an integrity technique is indeed required. The digital documents includes digital signature have the same problem also. Since, Verify the digital signature is necessary thing that conducted with a public key certificate signed by corresponding private key to sign. The digital signature is impossible to confirm if it is generated during the validation period of the certificate during the certificate expires or revoked (Ansper, 2001), (Stuartr, Kaliski and Stornetta,1995), (Surety, 2001).

This is because there is no insurance of private key validation when the certificate expire. Since, the certificate validity period is ranged from (1-2) years in general. Therefore, to keep the digital data and It's corresponding digital signature secure for a long decade a time-stamp techniques. time-stamp is used to prove the validity of a

*Sahar Adill Kadum

Email addresses: wsci.saha

Communicated by 'sub etitorr.adil@uobabylo.edu.iq' generated digital signature for a long time through validation process. A timestamp optimizes for certain data to exist before a specific time. Although, deals with the drawbacks of digital documents (Ansper, 2001), (Stuart, and W, 1991) .

Timestamp technology is a set of procedures that provide to the digital documents a long authentication in the time they were sent. The timestamp is an integral part of the legitimate infrastructure for digital documents, it enables proof of the document's existence at a particular time. It also helps to decrease the level of trust currently required for a public key by allowing proof to the document that was signed before the revocation procedure of the corresponding signing key is sealed. All of these facilities rely on timestamps to handle the documents and their signing keys validity status, to motivate the need for a clear understanding of the security and efficiency requirements of timestamps (Stuart, and W, 1991), (International Organization for Standardization, 2000), (International Organization for Standardization-part1, 2000). This research concerned with the time signature distributed scheme as a one of the time-stamp schemes.

2. Distributed Time Signature Scheme

The issuer of distributed time signature scheme deals with two types of servers: a reception server and multiple sign servers as depict in Fig (1). The scheme proposed by Takura et al. (1999).

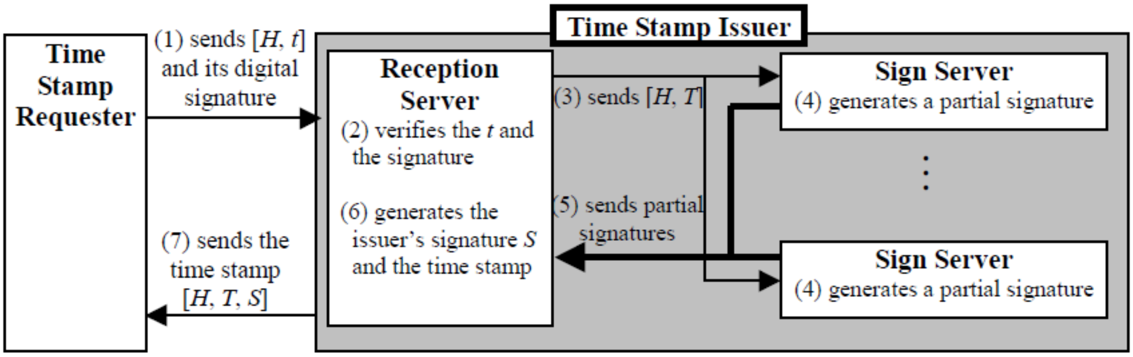
Time Stamp Requester
(1) sends [H, t] and its digital signature
Time Stamp Issuer
Reception Server
(2) verifies the t and the signature
(6) generates the issuer's signature S and the time stamp
(3) sends [H, T]
(5) sends partial signatures
Sign Server
(4) generates a partial signature
Sign Server
(4) generates a partial signature
(7) sends the time stamp [H, T, S]

Fig. 1- Time Signature Distributed Scheme

2.1 The issuing procedure:

Requester sends an issuer (H, t), S, [H: is a hash value of data, t: is the valid period of data, and S: is a digital signature of (H, t).

The receiving server receives the data to verify the signature and to ensure the period validity does not expire at the verification time. the receiving server sends it to the signature servers (H, T), each one contains partial data of a private key to construct digital signature. The server partially generates the signature on [H, T] during the current time process T and returns this signature to the receiving server. If the number of the received signatures is more than a threshold, then receiving server can generate a digital signature S and receive the requestor TS (H, T, S) [TS: is a timestamp] from the receiving server. Using the partial digital signature with a threshold be a big hindrance to the issuer to fraudulently tamper with the processes that create a timestamp (International Organization for Standardization-part1, 2000), (Une, Masashi, and Matsumoto, 2001), (Karel, 1995).

2.2 The verification procedure:

The validator verifies that the digital signature done by the issuer. Thus, the verification process is the verification of the digital signature by the issuer which corresponds to a process **b** (the Une and Matsumoto verification processes). The validator confirms between the data to be verified and the hash value in the timestamp, the process is implicitly included in the verification procedure. As a result, the validation procedure is corresponded **ab** process (Une and Matsumoto validations). Figure 1 shows that type **ab** belongs to class 2 (relationship of the Une and Matsumoto classes).

A sufficient condition conforming to category 2 is a technique to create an InfoINT (information integrity) that does not become vulnerable and the attacker does not collude with the issuer (International Organization for Standardization-part1, 2000), (Une, Masashi, and Matsumoto, 2001), (Karel, 1995).

3. Proposed Synchronizing Time Signature Distribution Scheme

To overcome the gaps of the distributed time signature system, he proposed a new configuration called "synchronization process". With this process and multiple signal servers that provide a partial signature, the process that sends its signature is periodically synchronized to one of the signature servers at random to obtain a timestamp (TS) for the signature. This connection between servers makes it difficult for each server to cheat in the TS. This makes the synchronization process work as a supported base for the distributed system to be more trustworthy as shown in Fig. 2.

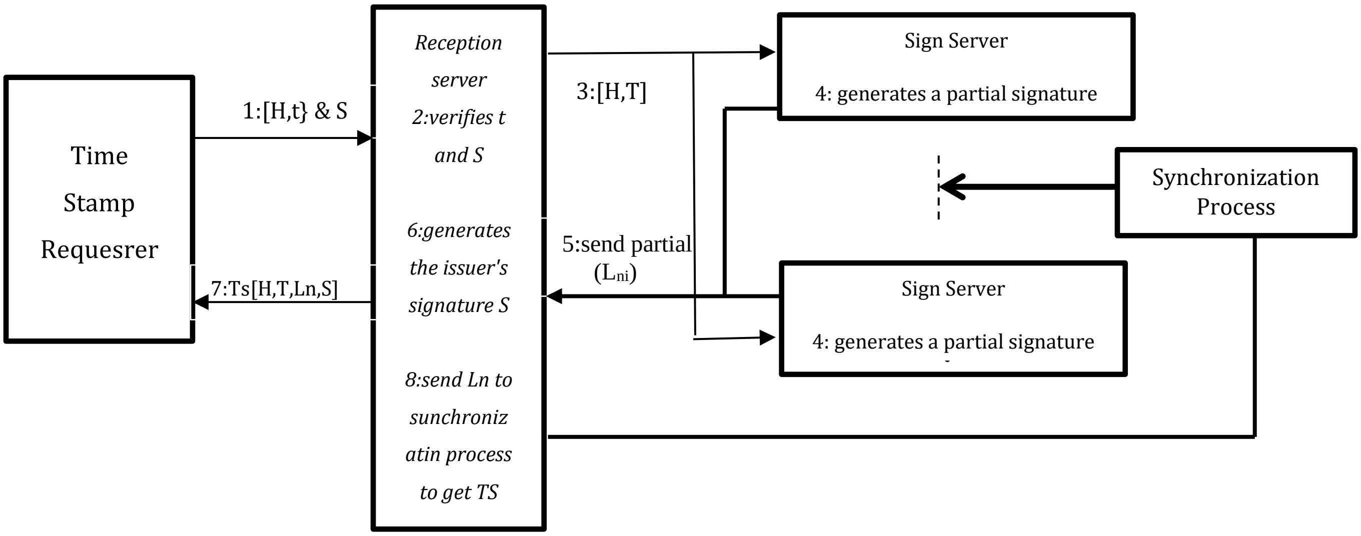
Time
Stamp
Requesrer
1:[H,t} & S
7:Ts[H,T,Ln,S]
Reception server
2:verifies t and S
6:generates the issuer's signature S
8:send Ln to sunchronizatin process to get TS
3:[H,T]
5:send partial (L_{ni})
Sign Server
4: generates a partial signature
Sign Server
4: generates a partial signature
Synchronization Process

Fig. 2- Synchronizing Time Signature Distributed Scheme

The issuance procedure is the same as the previous one except for the last step when the receiving server sends a timestamp to the requester, the timestamp contains H, T, Ln is a data set of (partial signature: -1, n + 1, T_{n-1}, H_{n-1}, and hash value L_{n-1}), and S.

In the synchronization process, the receiving server requests the binding information stamp (L_{n+k}) from one of the recording servers to obtain the TS (L_{n+k}).

3.1 Verification procedure

The verifier compares the hash values of the data to be verified with Hn and performs the verification of the digital signature S. These operations correspond to operations **a** and **b**, respectively. Then, the validator obtains a string of timestamp [TS_{n+1}, TS_{n+2}, ..., TS_{n+k-1}], and regenerates a string of link information [L_{n+1}, L_{n+2}, ..., L_{n+k}]. to confirm between them. [TS_{n+1}, +2, ..., TS_{n+k-1}] dataset (data used to ensure consistency between the timestamp data and the corresponding data in the issuer database).

One of time stamp entities is ETSI, the "TSI" of ETSI is the Issuer Time Stamp that keepet by the issuer), the **d** operation is the corresponding operation (Une and Matsumoto verification operations). Finally, the verifier obtains TS(L_{n+k}) from reception server and compares between L_{n+k} and the regenerated one. The corresponding operation is **e** (Une and Matsumoto verification operations) because TS(L_{n+k}) and reception server correspond to EAMP (Evidence Amplifier) . the EAMP is a data used to confirm the integrity of ETSI and send to an evidence amplifier by an issuer. The "AMP" of EAMP means "AMPlifier", the evidence amplifier keeps EAMP to be verified during the verification phase and amplifier, respectively. Thus, the scheme correspond to **abde** type and class 6 (Une and Matsumoto groups of time stamp schemes).

4. The Effect of Synchronization Process

The following points resulted from the first distributed time signature scheme in security evaluating:

- Firstly, checking whether it is infeasible or not to the attacker to forge the digital signature without using the sign servers partial private keys.
- Secondly, checking the receiving server and signing servers if they are trustworthy enough to ensure that

synchronize the partial digital signature and threshold configure a difficulty for the issuer to fraudulent the operations involved in creating a timestamp. A sufficient condition for the security of a trust to be achieved is the combination of the following three conditions:

- first: InfoINT generation is not vulnerable, and the attacker cannot collude with the issuer.
- Second: The attacker does not conspire with the issuer and does not impersonate him.
- Third: The attacker does not conspire with a amplifier and does not impersonate him.

5. Conclusion

Implementing the proposed synchronizing the partial digital signature with a specific threshold configure a big difficult to the issuer to defraud the operations involved in timestamp creation. Although adding two operations to the verification process makes forging the digital signature used in the new scheme impossible for an attacker and makes the receiving server and signaling servers trustworthy enough to perform fraudulent manipulation of any operations related to the scheme.

References

[1] Ansper, Arne, AhtoBuldas, MärtSaarepera and Jan Willemson, “Improving the availability of timestampingservices,” *Proceedings of ACISP2001*, LNCS 2119, Springer-Verlag, (2001), pp:360-375.

[2] Stuart. Haber, Kaliski. Burt and Stornetta.Wakefield Scott ,“How Do Digital Time-Stamps SupportDigital Signatures?”,*CryptoByte*, 1 (3), (1995), pp.14-15, (http://www.rsa.com/rsalabs/.

[3] Stuart. Haber, W. Scott, "How to Time Stamp Digital Document", journal of cryptology, vol:3, no:2, (1991), pp: 99-11.

[4] International Organization for Standardization and International ElectrotechnicalCommission,ISO/IEC JTC 1/SC 27,"Information technology-Security techniques", Germany Din, (2000).

[5] International Organization for Standardization and International ElectrotechnicalCommission,*ISO/IEC Working Draft 18014-1: Information technology - Security techniques -Time stampingservices -Part 1: Framework*, http://csrc.nist.gov/cc/t4/sc27/post-londonfiles/27n2595.pdf, (2000).

[6] Surety.com; "*Secure Time/Data Stamping in a Public Key Infrastructure*", http://www.surety.com/home/pki.pdf, 2001.

[7] Une, Masashi, and Matsumoto. Tsutomu, “Relations between Security and Verification Procedures ofTime Stamps",*Proceedings of the 2001 Symposium on Cryptography and Information Security*,The Institute of Electronics, Information and Communication Engineers, (2001) pp.629-634.

[8] Karel. Wouters, " Time-Stamping: a survey", (1995), Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=07147a4bfe6f61901a953c52ab29fcf2cfde2cf3