Reliable Clock Synchronization for Electronic Documents

Júlio S. Dias[2*], **Denise B. Demétrio**[1] , **Ricardo F. Custódio**[1] , **Carlos R. De Rolt**[2]

[1]Laboratório de Segurança em Computação – Universidade Federal de Santa Catarina

[2]Universidade do Estado de Santa Catarina

jdias@inf.ufsc.br, denise@inf.ufsc.br, custodio@inf.ufsc.br, rolt@udesc.br

Abstract. *Trusted time sources are required to insert time stamps in electronic documents. A signed and time stamped electronic document is equivalent to a traditional paper document and is legally recognized. Clock synchronization protocols of the sort provided by Network Time Protocol (NTP) do not satisfy all requirements to assure that a time source is trustworthy. This paper proposes the use of an external Certificate Authority (CA) to issue digital certificates to all computer systems that want to synchronize their clocks using NTPv4 protocol. The use of external auditors and a Time Stamp Authority (TSA) based on relative techniques to make this kind of service trustworthy is also proposed. All modules inserted will not affect the normal operation of NTP protocol.*

Keywords: Security Management, Clock Synchronization, NTP auditing.

1 Introduction

Electronic documents are used in information systems, data communication and electronic commerce. Their use is possible with authenticity, integrity, non-repudiation and time related evidence requirements assured. The authentication and integrity are constructed with cryptographic methods such as hash functions and digital signatures [Stinson, 2002, Menezes, 1997]. The non-repudiation requirement is claimed technologically to be fulfilled through authentication but this approach is not widely accepted and will not be discussed in this paper [Balacheff et al., 2001]. The time related evidence is achieved through temporal information that presents the time instant at which events relative to documents, and the computer systems utilized in their processing, occurred. The temporal anchor, time related evidence, is a precise time at which the existence of an electronic document can be proved and also that it has not been modified since that time. This time related evidence is provided by a trustworthy third party entity that issues a time stamp. This entity is called a Time Stamp Authority (TSA) [Buldas et al., 1998, Pasqual, 2002] that supplies part of the legal and technical infrastructure to allow wide use of electronic documents. Therefore the use of a trusted third party, like TSA, has been recommended to add trust to electronic documents [Müller, 2000] and a time stamped and signed document provides the trust anchor that is necessary for the document to be legally valid [Bortoli, 2002]. The TSA must supply the correct time and date when issuing time stamps. This subject has stimulated the scientific community to study new ways to issue time stamps and trustworthy clock synchronization of computer platforms. The clock synchronization is important to overcome weaknesses presented by computer system time keeping techniques. According to Lombardi [Lombardi, 2000], the currently used computer systems present two ways to keep time information: hardware and software clocks. The software clock is responsible for keeping time information when the computer is running. Only the hardware clock is running when the computer is turned off. When the computer starts up, the operating system makes the adjustment to the software clock by reading the current time that is supplied by the hardware clock. This approach does not show good performance in relation to stability over time and with varying temperature leading the computer clock to present unacceptable delays. The time anchor of an electronic document cannot be subjected to such variation. To solve this and other problems related to time keeping of distributed computer systems it is necessary to synchronize their clocks with trustworthy time sources. The time information would be relayed from these sources to all entities requiring their clock to be synchronized. There is not a widely accepted solution to reliable and secure clock synchronization.

The importance of time keeping techniques and clock synchronization has lead to development of legislation and recommendations by many governments. These legislators and governments are worried about how to disseminate legally recognized signals for frequency and time synchronization to be used in many applications and systems such as Time Stamp Authorities, Public Key Infrastructures and Digital Signature Software [Brasil, 2001, Federal, 2002, ICP-Brasil, 2002].

The aim of this paper is to propose an audit system for a trustworthy and secure clock synchronization system. This will permit the traceability for time supply. The traceability permits the confirmation of the time source used in the electronic

[*] Supported by Santa Catarina State University and CAPES.

document processing or signing. The system is based on NTPv4 protocol which achieves clock synchronization and some authentication level. An alteration in NTPv4 relating to the protocol security model is also proposed in order to achieve reliable authentication of entities participating in the clock synchronization process. This alteration consists of adding an external Certificate Authority to allow authentication and easier management of digital certificates used.

Section 2 presents a revision of time stamp methods. Section 3 presents a survey of the main protocols used in clock synchronization of computer systems with particular attention to NTPv4 that is used as a base in the secure clock synchronization system. In section 4 a proposal for an audit system for clock synchronization which achieves the required features is presented. Section 6 presents final considerations with respect to the system developed.

2 Time Stamp Methods

The use of electronic documents and digital signatures is possible with security requirements fulfillment as stated above. This work is about how to supply trusted time related evidence to this kind of document through the use of reliable clock synchronization structure. This section presents the methods used by Time Stamp Authorities when time stamping electronic documents.

The time stamp methods are supposed to fulfill the following security requirements [Haber and Stornetta, 1991]:

Privacy: Only the document owner must have access to the document content;

Communication channel and storage: It must be practical to time stamp a document regardless of its size;

Communication Failure: It must guarantee the integrity of data sent over communication links and the continuous operation of the system;

Confidence: It must guarantee that the TSA will time stamp the document with the correct date and time;

Non-repudiation: It must guarantee that the TSA will not repudiate its actions;

Anonymity: It must not be able to associate a time stamp request to a customer.

The methods based on a Trusted Third Party are the most appropriate to fulfill the requirements above. The privacy, communication channel and storage can be fulfilled through the use of hash functions and digital signatures. The hash functions are procedures that map a document of any size as a fixed size sequence of bits, like MD5 and SHA-1, which respectively produce hashes with 128 and 160 bits. Instead of transmitting the document, the customer transmits the hash function result, which is smaller than the original document, meeting the privacy and communication channel and storage requirements.

Another improvement that can be accomplished is to add a digital signature to the scheme. When the document hash arrives to be time-stamped, the Time Stamping Authority attaches the date and hour to the hash, signs it and sends it to the customer. The customer verifies the signature and certifies that the hash received is the same that was sent to the Time Stamping Authority fulfilling the avoidance of communication failure requirement.

Anonymity can be achieved through mix nets [Chaum, 1995], onions routing [Goldschlag et al., 1999], web mixes [Berthold et al., 2001] or crowds [Reiter and Rubin, 1998]. The anonymity hides the client identity from the Time Stamp Authority. This is a security requirement that is not necessary for all applications such as billing systems where authentication is required.

The confidence and non-repudiation are related to the temporal question, that is, how the document receives the data and hour. It could be **absolute**, **relative** or **hybrid**. Absolute time stamp methods issue time stamps using local machine clocks as a reference. Relative time stamp methods issue time stamps containing information that only verifies if a document was time stamped before or after another document [Roos, 1999, Just, 1998], using an approach similar to Lamport logical clocks [Lamport, 1978] where is not important on obtaining and maintaining true time but the order in which events occur. In hybrid methods absolute and relative characteristics are presented. When using absolute methods, physical access restriction and auditing procedures can be used to fulfill confidence and non-repudiation requirements but this procedure will only delegate the trust to another entity, the Auditor. In the relative and hybrid methods a trustworthy Time Stamp Authority is not required because there are mechanisms which guarantee that a document will always be time-stamped with the current date and time even if the Time Stamp Authority is malicious [Roos, 1999, Haber and Stornetta, 1991].

To achieve the confidence and non-repudiation requirement, the Time Stamping Authority could link all the submitted hashes in a chain using a hash function *H*. In this case the stamp *s* for the n-th document H_n would be [Lipmaa, 1999]:

$$s = Sig_{TSA}(n, t_n, ID_n, H_n, L_n) \tag{1}$$

where Sig_{TSA} is the Time Stamp Authority digital signature, t_n is the current document date, ID_n is the identification of the n-th document and L_n is the link information:

$$L_n = (t_{n-1}, ID_{n-1}, Hn - 1, H(L_{n-1})) \tag{2}$$

where t_{n-1} and ID_{n-1} are the date and the identification of the previous document, H_{n-1} is the hash of the previous document and $H(L_{n-1})$ is the hash of the link information of the previous document. Figure 1 shows what the linking of 9 elements would be like.

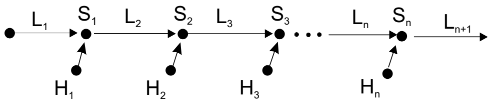

Figura 1: Linking scheme.

In this way, the Time Stamp Authority associates the current stamp with the previous one to get a stamp sequence with inbound order, resolving dispute problems, since the Time Stamp Authority can identify if a document was time stamped before another one through the chain tracking.

This approach presents limitations with respect to time spent in verifying the relation between the two stamps, that is directly proportional to the number of linked stamps in the chain.

New methods have been proposed to solve the problems presented by linking schemes. The synchronized tree method is an efficient linking scheme that can be assembled, to reduce the obtention time of an individual stamp. Considering that all the hashes which arrive to be time-stamped are linked, and that at the end of a certain time a function *F* is applied to all those hashes to generate a single stamp that represents them, the following scheme can be built:

1. The customer who wants to protocol his document, produces a hash and sends it to the Time Stamp Authority;
2. When a hash arrives to be time-stamped, it is link with the other requisitions, through a function *F* ;
3. At the end of each round, for example 60 seconds, the function *F* is applied again to the last element of the chain and to the stamp of the previous round, these generate the current stamp of that round, as shown in figure 2.

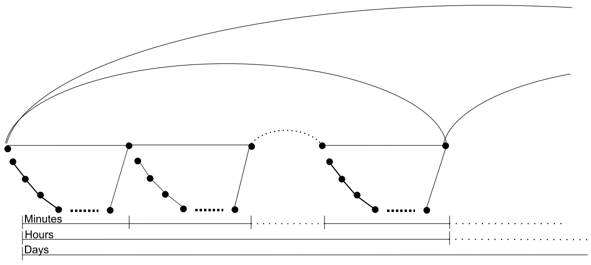

Figura 2: Generalization of the scheme.

Each H_i is the representation of each hash submitted to the Time Stamp Authority and linked to a function *F*. R_0 is the stamp of the previous round and R_1 is the current stamp of the round and so on. Generalizing the process, larger rounds can be created, representing known units of time like hours, days, months and even years, to reduce the verification time of documents. This generalization can be seen in the illustration 2.

The verification can be accomplished searching the formed tree, according to the date and value of the stamp produced. For example, a document which was stamped on 22/03/2001 and at 14:32 PM, the order of verification will be: year, month, day, hour, minute and then the document hash is verified. It is important to remember that all the methods mentioned above, as well as this one, publish all the stamps in a public directory.

This method was proposed and developed by Pasqual [Pasqual et al., 2002] and is called the Synchronized Tree. The method uses a hybrid approach to issue time stamps. It also presents other schemes to aggregate trust during the process.

3 Clock Synchronization Protocols

The need for clock synchronization has lead to the development of many technologies and protocols. The existing methods of clock synchronization differ basically in the resolution and the communication medium used to signal propagation. The technologies developed allow that such a task can be achieved with success independently of the communication medium and localization of the parts. Currently, the distribution of time information can be achieved through the use of radio signals, telephone lines or data communication networks such as the Internet [Lombardi, 2000].

The protocols and techniques IRIG [IRIG, 1987], WWVH, WWVB, GPS [Allan and et All, 1998] use radio frequencies, ACTS [Nist, 2000] uses a telephone network and the NTP protocol family [Postel and Harrenstien, 1983, Mills, 1992, Mills, 2002c, Mills, 1996] uses data communication networks to allow clock synchronization. The principal motivation to continue using the ACTS, IRIG and GPS protocols is the trustworthiness of the time source. In these protocols, the client trusts in the supplier, despite the high cost added. It is believed that the NTP protocol will replace these protocols as a great amount of trust will be added.

The protocols based on radio frequency need receptor equipment and antennas. This equipment presents high cost to acquire, operate and perform maintenance. The ACTS protocol needs only a modem; however, to achieve clock synchronization, it is necessary to establish a dial connection that may be a long distance call, not economically acceptable in many applications.

Data communication networks based on TCP/IP protocol, like the Internet, are found all around the world and naturally became the chosen communication medium to allow clock synchronization. In order to make use of this medium, many clock synchronization protocols were developed, among them the following can be cited: Time Protocol, Daytime Protocol, Network Time Protocol-NTP and Simple Network Time Protocol - SNTP. The most used protocol currently is the NTP [Mills, 1996].

The NTP protocol is used to achieve clock synchronization between a trusted time server and clients [Deeths, 2001]. NTP was developed based on the principle that all machines must present a time as close as possible to the correct time. It is designed to achieve a precision of milliseconds in Local Area Networks without too much network equipment, such as routers. The NTP protocol uses a stratum concept, that is, a hierarchical model with each server on one level or stratum serving as a server to lower levels. The lower the client in the hierarchy the higher its stratum will be. A time server attached to a trusted time source is termed stratum 1 server while the time source itself is termed stratum 0. The highest stratum acceptable is numbered 15. The trustworthy model offered currently by NTP consists of the use of several servers as clock synchronization sources. This architecture achieves reliability and greater precision. The failure or malfunctioning through malicious action of one or a few servers will not damage the synchronization scheme, because to damage the system it is necessary that most of the time servers are damaged and this is unlikely to happen. The malfunctioning servers are taken out without any loss to the synchronization. The discarding of servers that have incorrect data is achieved by clients through the use of statistical methods [Mills, 1997]. Message time stamps are also used to make NTP resistant to replay attacks. The figure 3 presents a typical NTP hierarchy. The NTP protocol states that communication between NTP entities can present different modes. The most used association modes are presented below:

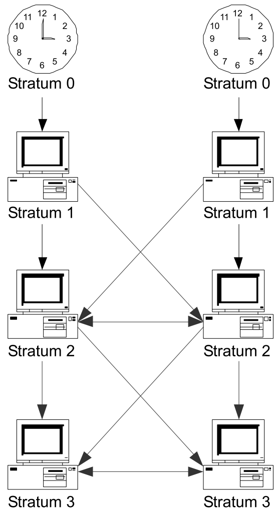

Figura 3: Typical NTP Hierarchy

Client/Server where a client entity always requests clock synchronization from a time server presenting the lowest stratum possible;

Peer to Peer where an entity can act as client or server with respect to its position to trusted clocks;

Multicast/Broadcast where automatic client or server clock synchronization is performed through multicast or broadcast messages.

Since version 2, NTP has been concerned about the authentication of the entities involved. In version 2, a rudimental authentication mechanism was defined, based on an access list. This list, maintained by the server, contains the IP addresses of authorized clients. A more elaborate scheme of authentication is based on symmetric cryptography and is included in all versions after version 2. In this scheme, the server generates a symmetric keys list. The keys are distributed to all clients that will use the service, permitting the entities involved to authenticate and verify the integrity of their communication. To exchange messages, the protocol determines that it should calculate the package hash, it ciphers the package with the secret key and attaches it to the message. In this way, the messages exchanged between clients and servers have the integrity and authenticity guarantee supplied by the use of the key that only the entities involved know.

However, this scheme presents a key distribution problem. To solve this problem the Autokey protocol was introduced, in version 4 [Mills, 2002b]. The Autokey protocol uses digital certificates to identify the servers. Digital certificates are electronic documents signed by a Certificate Authority that contain the owner name, the sender entity, the owner public key and the certificate validity period. In the NTPv4 self-signed certificates are used.

The NTP protocol with Autokey [Mills,] presents the follow steps:

- The server S generates a self-signed digital certificate;
- The client C copies the S certificate or requests it through an appropriate message. In case of a request, C must have the IP address of S. When C receives the certificate, it verifies whether the certificate name matches that registered for the sender IP, through the use of DNS protocol;
- After C receives the server information, C sends a cookie request, that is, information that will be used while the entities are associated.

- S calculates the cookie based on public information (clients and servers IP, key identification to be used) and random numbers and sends it signed to client;
- C verifies the digital signature and generates the keys list to be used in communication;
- When both parts possess the common symmetric keys, there is a situation where only information exchange is necessary to synchronize the C clock.

However, NTP still does not require authentication of clients that request clock synchronization from time servers. This authentication would be used to provide traceability from clients to servers. Any server or client in the NTP hierarchy would be identified and would not be able to repudiate its actions.

The NTP, in all of its versions, does not include an audit scheme. The auditing information can only be obtained from the computer logs stored by servers in the hierarchy. This lead some companies to propose alternative audit schemes for time distribution systems. The audit system of Wetstone (www.wetstonetech.com) and Symetricon (www.symetricon.com), carries out periodic verifications and maintains registers of events, issuing certificates of guarantee to the parties involved. Regarding the systems developed it is stated that:

- Guarantees that all elements involved are synchronized with a trustworthy time source;
- Guarantees that the time information was not manipulated in a malicious manner;
- Creates evidence that guarantees the irrefutability and traceability of events.

However, this audit system has vulnerabilities, principally:

- A server to be audited knows the auditor identity and can work in a malicious manner;
- The events are registered by absolute time stamp, which does not guarantee the traceability of events, as was explained in section 2. The parties acting in a malicious manner can add events later on;
- There is no trustworthy authentication scheme;
- The clients are at a disadvantage, because it is not possible to prove their honesty to malfunctioning servers or auditors.

It was shown that NTP was developed in order to present precision and resolution in clock synchronization [Mills, 2002a]. However, there are applications where traceability of time to reliable sources is necessary. The NTP protocol cannot prove that the correct time was employed by clients and servers. It may be that the server synchronized its clock from a trustworthy time source, but subsequently used another time to perform its activities.

Therefore, we have proposed the supply of additional functions outside the original specification, without changing its normal behavior. In the following section the system proposed to overcome NTP security limitations will be shown.

4 Access Protocol and Auditing System

The proposed architecture presents a system where all the entities are identified and have their clocks audited by an external auditor. The use of a system similar to conventional NTP hierarchy shown in figure 4, is proposed, including the following entities:

Auditor: Entity responsible for the control of all entities that use NTP for clock synchronization. Auditing modules allow greater control without loosing the resolution and precision supplied by the original NTP implementation;

TSA: Entity responsible for time stamping electronic documents. The time stamped documents are responses to requests sent by the auditor to other time servers and are audit trails from all the entities in the hierarchy;

CA/CRL: Services which are part of the public key infrastructure for the entities present in the NTP hierarchy. External Certificate Authorities are utilized to allow authentication of entities participating in the NTP hierarchy. All participants must present digital certificates issued by this external CA. The use of an external CA will provide greater reliability between peers.

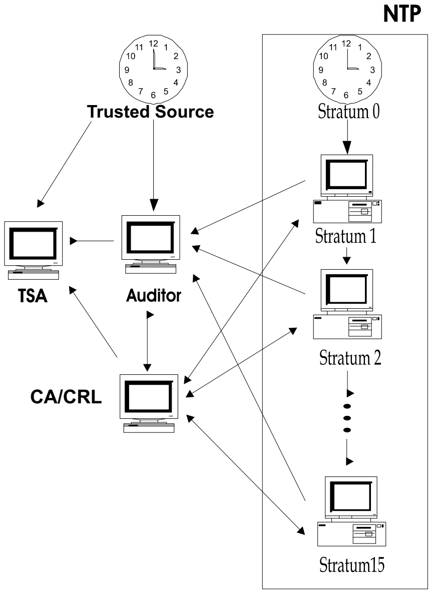

Figura 4: Auditing System Architecture.

The proposed auditor will be anonymous, and will not be recognized as an auditor by other entities in the hierarchy. The use of an anonymous auditor will make it difficult for fraudulent time servers to operate within the hierarchy. The auditor will periodically require time information from other participating entities. This information will be stored and analyzed, providing evidence to identify the potentially malicious elements. The auditor, through a knowledge of the structure of the hierarchy can provide the traceability information necessary in a legal dispute.

Taking into consideration that the actual auditor could be capable of malicious behavior, a TSA was added. The data collected are all time stamped and use the hybrid methods (relative and absolute). The utilization of the Synchronized Tree Protocol guarantees the impossibility of fraud on the part of the auditor. It is not possible for the auditor to change the data collected without being discovered.

The auditor and TSA clocks are synchronized directly from a primary time standard(s) or a set of trustworthy time servers.

An essential element for the present proposal is the utilization of an external CA. This CA guarantees the identity of the entities involved in the clock synchronization process. Only elements that have a valid digital certificate are considered trustworthy and can access the clock synchronization services. The mutual authentication carried out at the moment of the confirmation of an association between the clients and servers allows the clock synchronization services to be executed. The utilization of certificates issued by a trustworthy external CA reinforces the control over entities using the system.

The auditor having verified that an entity is behaving abnormally, and having proved an attempt of fraud on the part of the entity, requests from the CA the revocation of the digital certificate from the malicious entity, it thereby being excluded from the clock synchronization process.

An entity can request the services of a TSA to guarantee the time information relating to specific events. This provides proof that an entity did not act in a malicious manner. Any abnormal behavior observed on the part of one entity may in fact be due to that of another. The register keeping all of the requests that one entity sent to other participants, as well as their responses, provides evidence to find the malicious entity.

The mechanism is coupled with a NTPv4 protocol module. In this way the mode of functioning previously established by NTP is not altered, only new functions are added. It is important to highlight that NTP clients and servers, even if they are not identified by the Auditor, can take part in clock synchronization, naturally conforming with the NTPv4 protocol. However, these entities will not provide a certified and trustworthy time service.

The developed architecture presents as principal characteristics:

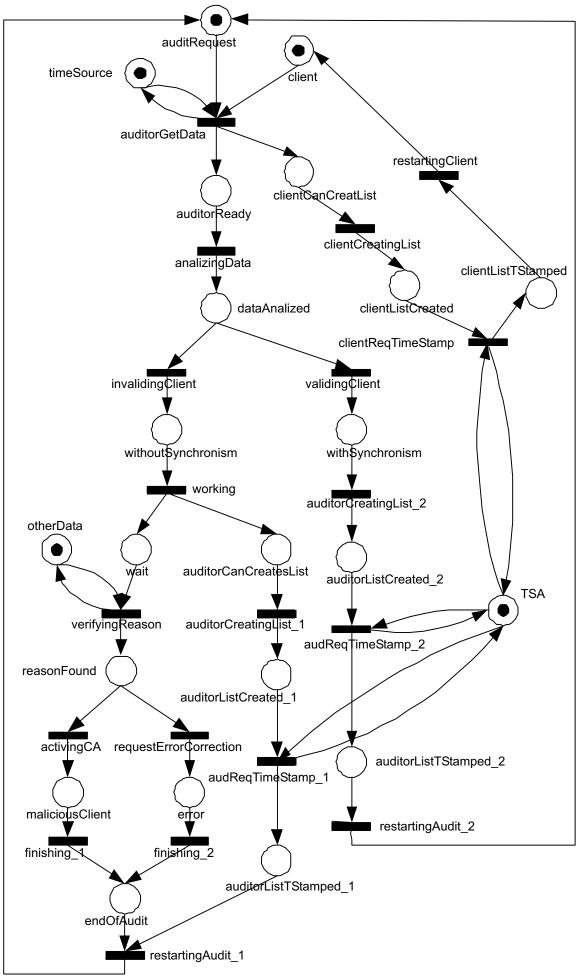

Figura 5: Petri Net Model.

- The use of anonymous auditors, making it difficult for malicious entities to identify them;
- The use of a TSA which utilizes the Synchronized Tree Method, making it difficult for the auditor to fake the results of the auditing process, by inserting data after the time of collection;
- The use of digital certificates issued by an official external public key infrastructure, adding confidence to the clock synchronization process;
- The use of a Certificate Revocation List - CRL to guarantee the quality of the services provided by the system.

5 Security Analysis

The system was proposed and developed in order to fulfill security requirements necessary for the use of the NTPv4 protocol in applications where mutual authentication is required. In a typical configuration the servers are not under a common administration, and it is not easy to carry out a trace from the reliable time source to any client in the NTP hierarchy. The information provided by the servers cannot be trusted and the auditing process is required to reinforce NTPv4 security requirements.

The NTP protocol provides several levels of defense against attacks. The auditing system proposed is inserted within the NTP maintaining the original security properties of the protocol.

The system was formalized and validated using Petri Nets as shown in figure 5, which provides a model which is used to validate the states assumed by the entities participating in the hierarchy.

We used Petri Nets [Murata, 1989] as a first step to guarantee a reliable system. We have validated the software under development. The Petri Net resulting from the modelling process has been processed by ARP (http://sourceforge.net/projects/jarp/). The processing of the model has presented a reliable, deadlock free system.

The protocol was also validated using GNY logic and Isabelle theorem prover [Paulson, 1997]. We have used inductive methods to validate the protocols used to authenticate and request for services. We have found that the security properties such as authentication, non-repudiation and message integrity were achieved.

6 Conclusions

The growing use of digital time stamp services creates a demand for reliable and efficient methods. Besides time stamp methods it is necessary to supply reliable clock synchronization for trusted time stamp operation.

The review of time synchronization protocols and techniques presented weaknesses with respect to the auditing process and the authentication of entities participating in the hierarchy. It is known that clock synchronization alone does not assures a trusted system. The auditing system proposed and developed provides traceability of time dissemination from trusted time servers to the clients. This process adds trust to the clock synchronization process.

The authentication provided in current protocols such as NTP does not fulfill security requirement and does not allow the Auditor to identify all entities participating in the hierarchy through a formal process. The use of Certificate Authorities external to NTPv4 achieving mutual authentication, where clients and servers must provide their identification to each other, allows better management and the control of time servers and clients by the Auditor.

The system proposed guarantees the dissemination of time information in a safe and trustworthy manner, providing the time related evidence that can be used to confirm the origin of the time used in the electronic transactions.

The system was designed to not change NTPv4 behavior. This objective was achieved in our first version where the new functions inserted did not change the NTPv4 operation. The transition to the architecture proposed was not perceived by the entities.

The supply of a trustworthy time service is necessary to achieve greater confidence in the temporal anchor presented in electronic documents. The use of time related evidence provided by the proposed system can be of fundamental importance in the resolution of disputes. These dispute situations will be common as soon as the use of electronic documents and digital signatures has been established in computer systems and applications.

References

Allan, D. W. and et All (1998). The science of timekeeping. Technical Report 1289, Hewlett Packard.

Balacheff, B., Chen, L., Plaquin, D., and Proudler, G. (2001). A trusted process to digitally sign a document. In *Proceedings of the 2001 workshop on New security paradigms*, pages 79–86. ACM Press.

Berthold, O., Federrath, H., and Köpsell, S. (2001). Web mixes: a system for anonymous and unobservable internet access. In *Designing Privacy Enhancing Technologies*, pages 115–129. International Workshop on Design Issues in Anonymity and Unobservability.

Bortoli, D. L. (2002). O documento eletrônico no ofício de registro civil de pessoas naturais. Master's thesis, Curso de Pós-Graduação em Ciêncioa da Computação da Universidade Federal de Santa Catarina.

Brasil (2001). Medida provisória 2.200-2. Media Provisória que instituíu a ICP-Brasil.

Buldas, A., Laud, P., Lipmaa, H., and Villemson, J. (1998). Time-stamping with binary linking schemes. In Krawczyk, H., editor, *Advances in Cryptology – CRYPTO ' 98*, volume 1462 of *Lecture Notes in Computer Science*, pages 486–501. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany.

Chaum, D. C. (1995). Untraceable electronic mail, return address, and digital pseudonyms. *Communications of ACM*, 24(2):84–88.

Deeths, D. (2001). Using NTP to control and synchronize system clocks. Technical report, Sun Microsystems.

Federal, G. (2002). Decreto lei 4.264.

Goldschlag, D., Reed, M., and Syverson, P. (1999). Onion routing for anonymous and private internet connections. *Communications of ACM*, pages 39–41.

Haber, S. and Stornetta, S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3:99–112.

ICP-Brasil, C. G. D. (2002). RESOLUÇÃO no 16. Resolução que determina o Observatório Nacional como fornecedor da hora legal brasileira para a ICP-Brasil.

IRIG (1987). Irig standard 205-87. Range Commanders Council of the US Army White Sands Missile Range.

Just, M. K. (1998). *On the Temporal Authentication of Digital Data*. Ph.d., School of Computer Science - Carleton University.

Lamport, L. (1978). Clocks, and the ordering of events in a distributed system. *Communications of the ACM*, 21:558–565.

Lipmaa, H. (1999). *SECURE AND EFFICIENT TIME-STAMPING SYSTEMS*. Ph.d, University of Tartu - Estonia.

Lombardi, M. (2000). Computer time synchronization. Technical report, National Institute of Starndards and Technology.

Menezes, P. V. O. S. V. A. (1997). *HandBook of Applied Criptography*. CRC Press, Boca Raton, FL - USA, 1 edition.

Mills, D. Authentication scheme for distributed, ubiquitous, real-time protocols.

Mills, D. L. (1992). RFC 1305: Network time protocol (version 3) specification, implementation.

Mills, D. L. (1996). RFC 2030: Simple network time protocol (sntp) version 4 for ipv4, ipv6 and osi.

Mills, D. L. (1997). Authentication scheme for distributed, ubiquitous, real - time protocols. *Advanced Telecommunications/Information Distribution (ATIRP) Conference*.

Mills, D. L. (2002a). *NTP Documentation*. http://www.eecis.udel.edu/ ntp/documentation.html.

Mills, D. L. (2002b). NTP implementation manual. Publicado eletrônicamente no sítio. Visitado em outubro de 2002.

Mills, D. L. (2002c). RFC 2026: Public key cryptrography for the network time protocol.

Müller, R. (2000). ISO/IEC 18014-1: Information technology - security techniques - time stamping services - part 1: Framework. Norma Estabelecendo Time Stamping Services.

Murata, T. (1989). Petri nets: Properites, analysis and applicatons. *Proceedings of the IEEE*, 77(4).

Nist (2000). *Federal Emergency Management Information Systems*. NIST, Estados Unidos.

Pasqual, E. S. (2002). Idde - uma infra-estrutura para a datação de documentos eletrônicos. Master's thesis, Curso de Pós-Graduação em Ciêncioa da Computação da Universidade Federal de Santa Catarina.

Pasqual, E. S., Dias, J. D. S., and Custódio, R. F. (2002). A new method for digital time-stamping of electronic document. In FIRST, editor, *Proceedings of the FIRST 14th Annual Computer Security*, 212 West Washington, Suite 1804 Chicago, IL 60606. Phoebe J. Boelter Conference and Publication Services, Ltd.

Paulson, L. C. (1997). The inductive approach to verifying cryptographic protocols. In *Symposium on Security and Privacy*.

Postel, J. and Harrenstien, K. (1983). RFC 868: Time protocol.

Reiter, M. K. and Rubin, A. D. (1998). Crowds: anonymity for Web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92.

Roos, M. (1999). Integrating time-stamping and notarization. Masterthesis, University of Tartu - Estonia.

Stinson, D. R. (2002). *Cryptography – Theory and Practice*. CRC Press, Boca Raton.