

## Enhancing e-Government Services through Digital Time Stamping: Time Stamping System Specifications

prof. Rimantas Gatautis, Kaunas University of Technology, Kaunas, Lithuania, [rgataut@ktu.lt](mailto:rgataut@ktu.lt)  
 dr. Artūras Mažeika, Mykolas Romeris University and VMI, Vilnius, Lithuania, [arturasm@mrni.lt](mailto:arturasm@mrni.lt)  
 dr. Peeter Laud, Tartu University and Cybernetica AS, Tartu, Estonia, [peeter@cybernetica.ee](mailto:peeter@cybernetica.ee)  
 Rytis Satkauskas, Kaunas city parliament, [rytis.satkauskas@kaunas.lt](mailto:rytis.satkauskas@kaunas.lt)

### Abstract

*The paper aims to analyze the importance of digital time stamping service and digital time stamping systems components, organization requirements for implementing digital stamp service system. Time stamping helps significantly increase the level of confidence currently required in a public-key infrastructure by making it possible to track timing of signing the documents. Therefore time stamping in many cases is becoming ultimate evidence resolving the status of documents. The paper describes following Time stamping System components - NMI and TSU interface, Time stamping unit (TSU), Archive, User interface, Control system, VPN router. The paper reflects findings from EC funded 6<sup>th</sup> Framework project BALTICTIME (IST-027751).*

### 1. Introduction

The development of eGovernment services facilitate effective services providing for citizens, business enterprises or governmental organizations. The effective implementation of eGovernment services requires to process legally secure electronic documents and data files. That will enhance the security of electronic signature showing exactly when a document was signed, establishing an irrefutable sequence of events and also will contribute for development of fully online transactions environment as it requires multi level eSignature system. Much more technically secure and legally safe transactions over public open networks are a significant prerequisite for the further development of fully interactive electronic services. That will facilitate and accelerate the work of state institutions, create conditions for saving time and money, ensure faster, more convenient and efficient servicing.

In the context of development of eServices Digital Time Stamping service can play a significant role. Real importance of time stamping becomes clear when there is a need for a legal use of electronic documents with a long lifetime. During the last years, especially in the context of legal regulation of the use of digital signatures, the organizational and legal aspects of time stamping itself have become the subject of world-wide attention. Time stamping helps significantly increase the level of confidence currently required in a public-key infrastructure by making it possible to track timing of signing the documents. Therefore time stamping

in many cases is becoming ultimate evidence resolving the status of documents. The examples for use of time stamps can be validation of electronic signatures, computer logging (evaluation of performance and security issues in systems and networks), online subscriptions (granting revocation of subscriptions), digital notarization services, security policy/logins (additional level of protection), sales orders/receipts, content sealing, etc.

The use of electronic services and documents is becoming more and more frequent, presenting a series of advantages, amongst them, safer and faster communication, optimal use of resources and physical space, not to mention that they speed up the process.

In order to guarantee the integrity and the legality of such documents, techniques should be developed to simulate the traditional way of authenticating a document, that is, the electronic document should also be authenticated and signed. Along with the digital signature, the electronic documents begin to have a judicial value before a court of law, and are beginning to be used to solve disputes, in other words, Digital Time-Stamping guarantees the existence and integrity of one document at certain moment and the digital signature guarantees the connection between the document and the person who created it.

Introduction of the systems for identity management (eID, etc.) providing accountability and security for two-way interaction and higher online sophistication level services is one of the key factors for successful eGovernment public services acceptance. Time Stamping Authority (TSA) being integral part of the system is to large extent responsible for the confidence and accountability of these services. EC funded BALTICTIME project aims to develop the legal and accountable digital time stamping (DTS) system providing the layer of Trust in eGovernmental transaction environment and to demonstrate DTS system performance for time critical functions or validation data for digital signatures.

The main part of DTS is Time Stamping Authority (TSA). The functions of TSA are determined by the standard RFC 3161 [1]: “The TSA's role is to time-stamp a datum to establish evidence indicating that a datum existed before a particular time. This can then be used, for example, to verify that a digital signature was applied to a message before the corresponding certificate was revoked.”

The implementation and deployment of the BALTICTIME time stamping authority will enable the long-term validation (beyond the expiration of various signing keys) of digital signatures by allowing anyone to compare the times of creating the signature and the expiration of the signing key. Particularly in the eGovernment domain, the ability to ascertain the creation times of documents will enable the provision of the following services:

- Exchanges of documents in governmental and municipal organizations;
- Tax declarations;
- Public procurements;
- Electronic signature, public keys certificate authorities.

## 2. Linking-Based Time stamping

In a simple hash-and-sign time stamping the TSA receives the digest of a document, appends the current time to it and signs the resulting data structure. When the signing key expires, the timestamp loses its validity – we cannot verify whether the signature on the timestamp was created before or after the expiration. Linking-based time stamping allows the determination of the issuing order of two timestamps (but not the precise time of their issuing) even after the key used to sign the timestamps has expired. Moreover, linking-based time stamping does not allow even a malicious TSA to back-date documents (a hash-and-sign TSA can easily do that by including a wrong time in a timestamp).

Let  $T_1, T_2, T_3, \dots$  be the issued timestamps. Let  $X_i = h(T_i)$  be the digest of the timestamp  $T_i$ , where  $h$  is a one-way hash function, i.e. given some bit-string  $y$  it is very hard to find such  $x$  that  $h(x)=y$ . In linking-based time stamping, the time stamping server additionally constructs and stores the linking items  $L_i = h(X_i, L_{i-1})$ . In essence, the linking item  $L_i$  contains  $X_i$  and  $L_{i-1}$ , hence it cannot have been created earlier than them. By transitivity,  $L_n$  contains all  $X_m$  and  $L_m$  where  $m < n$ . The proof (called the linking chain) that  $L_n$  is later than  $L_m$  can also be presented – it consists of all  $X_i$  where  $m < i \leq n$ . With the help of those  $X_i$ ,  $L_n$  can be recomputed from  $L_m$ .

Similarly, we can present a proof that  $L_n$  is later than  $X_m$  for  $m \leq n$ . We use the existence of such proofs to show that one timestamp is earlier than the other one by letting each timestamp  $T_n$  contain the linking item  $L_{n'}$  where  $n'$  is smaller, but not much smaller than  $n$  (we can make  $n'$  equal to  $n-1$ ). In this way we can show that  $T_m$ , where  $m \leq n'$ , is earlier than  $T_n$  by showing that  $L_{n'}$  is later than  $X_m$ . Indeed, then  $T_n$  will contain  $L_{n'}$  that will in effect contain  $X_m$  that is the digest of  $T_m$ .

As hash-and-sign time stamping is unable to provide long-term integrity of timestamps, linking-based time stamping will be implemented in BALTICTIME. Still, signing the timestamps is

useful for including certain metadata with the timestamps, in particular the issuing time of the timestamp. Such signatures by themselves have a rather short validity period, but the links between the timestamps allow us to also convince ourselves in the validity of old timestamps, including their metadata. One of the effects of the linking is that each timestamp in some sense contains all preceding time stamps, hence the signature on a timestamp is also a signature on all previous timestamps.

If the linking-based time stamping is implemented as described above, then the verification of a linking chain between linking items  $L_m$  and  $L_n$  is of complexity  $O(n-m)$  which is definitely too much. Fortunately, if we let each linking item directly depend not only on the immediately preceding linking item, but also on a well-chosen earlier linking item, then the verification complexity can be reduced to completely acceptable  $O(\log n)$ .

## 3. Components of the Time stamping System

The structure and the hardware configuration of a Trusted TSA system are presented in Fig. 1. To cope with a large number of time stamping requests, we see the TSA to be deployed in a distributed manner, with one of the sites acting as a main system (TSA main site), keeping its time standards synchronized and its archive linked with the outside world (directly connected to the National Metrology Institute), while the other sites (TSA remote sites) synchronized and linked with the main site. A distributed system can also provide better availability which is important in time stamping applications where some party is always interested in obtaining the timestamp as soon as possible.

The main site of a TSA is composed of the following hardware components.

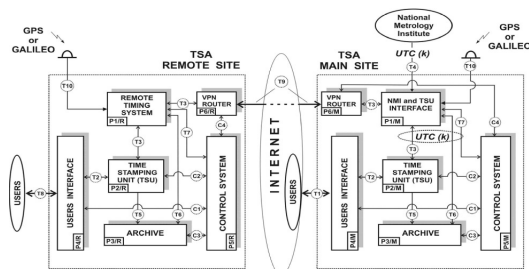
No.	Name	Purposes
P1/M	NMI and TSU interface	1. Time source for Time Stamps generation by TSU. 2. Warrant traceability of Remote timing system (P1/R) to the UTC(k) time scale. 3. Synchronize the TSA main site hardware components.
P2/M	Time stamping unit (TSU)	Time stamps generation
P3/M	Archive	Storage of issued time stamps
P4/M	User interface	Web service maintenance for small users
P5/M	Control system	Operation control of the TSA main site hardware components
P6/M	VPN router	Main and remote TSA sites secure communications

Figure 1: The structure and components of the TSA

The remote site of a TSA is composed of the following hardware components.

No.	Name	Purposes
P1/R	Remote timing system	1. Time source for Time Stamps generation by TSU. 2. Warrant traceability of remote timing system (P1/R) to the UTC(k) time scale. 3. Synchronize the TSA remote site hardware components. <b>Note:</b> Remote timing system is a part of NMI and TSU interface.
P2/R	Time stamping unit (TSU)	Generation of timestamps
P3/R	Archive	Storage of issued time stamps
P4/R	User interface	Time stamping service maintenance for big users
P5/R	Control system	Operation control of the TSA main site hardware components
P6/R	VPN router	Main and remote TSA sites secure communications

To allow the extraction of linking chains between timestamps issued by different sites (unless their times of issuance are very close together), the archives have to be synchronized with each other. Synchronization of archives really means that there are links between linking items in different archives. To create linking chains from already existing timestamps in archive A1 to future timestamps in archive A2, the archive A1 sends its currently last linking item L' to the archive A2. The archive A2 takes its last linking item Ln and computes  $L_{n+1} = h(L_n, L')$ . It also stores L'. A linking chain from an old timestamp in A1 to a new timestamp in A2 will pass through L' and  $L_{n+1}$ . The procedure just described creates "one-way" synchronization between A1 and A2. To get the synchronization also in the other direction, we repeat the procedure with the roles of A1 and A2 swapped. The frequency of executing this procedure gives the granularity of synchronization – if links between different archives are generated every t seconds then we are guaranteed the existence of a linking chain between the timestamps from those two archives if their issuance times differ by at least t seconds. To find this linking chain, the archive units must record which linking items have been used for synchronization.



If two timestamps are issued by two different TSUs almost simultaneously (less than t seconds apart) then there might exist no linking chain from one stamp to the other. In this case we cannot use linking items to show that one timestamp was issued before the other one. But we can still convince ourselves that both those timestamps have been issued later than some earlier timestamp, and before some later timestamp, thereby verifying their validity. The applications that check timestamps should gracefully handle such situations where two obviously valid timestamps with no linking chain between them have been presented. Such timestamps should be treated as simultaneous and if necessary, other criteria used to order them. Also, if the signature keys of the TSUs are still valid then the applications can extract the absolute times from the timestamps and compare them.

#### 4. Internal States of Components

##### 4.1. Time Mark Synchronization System

The time mark synchronization system keeps track of the current time traceable to UTC(k) and provides it to the all components of main and remote TSA sites. The key parts of time mark synchronization system are:

1. NMI and TSU interface;
2. Remote timing system.

##### NMI and TSU interface

Time Stamping Authorities will issue the legal Time Stamps (TS), id est TS should be traceable with UTC(k). The main purpose of NMI and TSU interface is to transfer UTC(k) time scale generated by Time Standard of National Metrology Institute (NMI) to the Time Stamping Units (TSU) of Time Stamping Authority. Other functions of NMI and TSU interface is the synchronization of all TSA components and warrant the remote timing system to the time Standard of NMI.

##### Remote Timing System

In order to provide required time accuracy (100 ms), and system autonomy for at least ten days the Timing Unit in the TSA Main or Remote Site should be equipped with at least 3 time standards which can provide frequency accuracy better than 10<sup>-8</sup>.

Considering price, and required accuracy rubidium frequency standards are recommended. Rubidium frequency standards provides frequency stability from 10<sup>-11</sup> to 10<sup>-12</sup>. Cesium frequency standards provide frequency stability from 10<sup>-13</sup> to 10<sup>-15</sup>, but are very expensive.

System based on three rubidium clocks after initial synchronization can work autonomously up to one year without external time comparisons to NMI (but it is not recommended). Using three clock provides the possibility of detection and elimination of bad-working clocks.

1PPS signal from time standards should be connected through multiplexer and time interval counter to Control Unit and compared continuously. Control Unit should be able to detect improper results from one of time standards, and eliminate bad-working time standard. In case when less than 2 time standards work correctly control unit should stop the time stamping process.

The Control Unit of the Timing System steers the direct comparisons of time standards, analyzes time standards parameters to select the master clock, and reads date and time data from time standards [2].

Control Unit, in order to determine time differences between master clock and NMI gathers and analyzes data from all time transfer method used to time synchronization, and every hour downloads GNSS data from GPS time transfer common view method

All important information are sent by Control Unit to Archive system and logged.

#### **4.2. Time stamping Unit**

In BALTICTIME, our plan is to use an existing, preferably open-source time stamping unit (TSU). Here we will describe the security requirements put on this TSU, as well as the parts of its state whose existence is dictated by the security requirements and the envisaged communication with other units according to BALTICTIME architecture.

Signature key and certificates for the public key  
Key management of the TSU is done according to the standard [5]. The certificates for the public key are distributed in the same way as certificates for signing keys of any other party. Some directory services may be used; or the certificate may accompany the signatures. The TSA signature key shall not be available in plain text and should be protected by a hardware security module. The backup and recovery of the TSA key will require multiple administrative users and the use of hardware security modules or smart cards to authenticate the individual administrators.

Last linking item

The TSU periodically queries the archival unit for the last linking item (or the archival unit periodically pushes it to the TSU). This linking item is included in the timestamps as a signed attribute. The linking item is a bit-string of the size comparable to the output length of hash functions.

In addition, the sequence number (in the archival unit) of this linking item is also stored.

#### **4.3. Archival Unit**

The archival unit keeps a log of time stamping server's activity, thereby allowing to audit it and to compare the timestamps after the keys used to sign them have expired. The archival unit also exchange the log items with remote archival units, thereby creating a single arrow of time, defined by the

collision-resistance of the hash function. Its state consists of the following parts.

The hash function

A cryptographically secure hash function  $h$  has been fixed. It is used to link the log items together. The hash function is not hardcoded, but the archival unit stores its identity. If necessary, the hash function may be changed (although this is supposed to be an infrequent and always an extraordinary event).

The chosen hash-function must be considered collision-resistant for the foreseeable future.

#### **The log**

The log is a set of items of the form  $(n, X_n, L_n)$ , where  $X_n$  is the  $n$ -th bitstring (timestamp) saved in the log and  $L_n = h(X_n, L_{n-1})$  is the linking information.

The log items may also need to store the source of the bit-string  $X_n$  (which may be the TSU, or the time mark synchronization unit, or the control system, or some remote archival unit) and the recipient(s) of  $L_n$ , if there are any (they may be the TSU or some remote archival units). Still, in this document we do not want to impose a requirement that such information must be saved or in what format and with how many details it has to be present. Hence this paragraph has to be treated as informational.

#### **Synchronization partners**

The configuration of the archival unit must include the addresses of other archival units, with whom the linking information is exchanged. For each archival unit we have to store its address (probably an IP address and a port number) and the frequency of synchronization.

#### **4.5. Control System**

The Control System component integrates all TSA components into unified system. The functions of the Control System are:

- Management of all TSA system devices;
- Monitoring of all TSA components and malfunction detection;
- Measurement and control of environment conditions;
- TSA users registration and controlling of access rights;

#### **4.6. Timing Unit of a Remote Subsystem**

We propose that the timing unit of the Remote Subsystem will use the same type of the time synchronization equipment as the main system (see Component for Time Mark Synchronization). Then, the timing data from Main Unit, used for the synchronization with the NMI, will also be used for the control of Remote Subsystem.

#### **4.7. Archival Unit of a Remote Subsystem**

The archival unit of a remote subsystem is identical to the archival unit of the main system.

### **5. Interfaces of Components**

#### **5.1. Time Synchronization Component ↔ NMI**

In order to provide required accuracy, and for security reasons all Trusted TSA must be synchronized to NMI using at least 2 different methods.

C/A multichannel GPS (in future GALILEO) common view method is recommended as primary

time transfer method. This method is not too expensive, and provides accuracy better than 5ns on distances up to 3000 km.

Network Time Protocol v4 is recommended as secondary time transfer method. It provides accuracy better than 5 ms. Time stamps in NTP should be authenticated using digital signature. NTP connection between NMI and TSA must be established using secure transmission channel (dedicated link, or VPN).

Time readings directly from GALILEO satellites should be considered in future as primary transfer method.

1PPS signal from master clock in NMI is connected to GPS/Galileo time transfer receiver, and NTP system.

1PPS signal from master clock in Trusted TSA is connected through multiplexer to GPS/Galileo time transfer receiver.

1PPS signal from GPS/Galileo time transfer receiver, and NTP system in Trusted TSA is connected through multiplexer, and time interval counter to control unit, and compared continuously to 1PPS signal from master clock.

Common view timing data are downloaded (using ftp- or http-protocol over VPN or dedicated link) by control unit in Trusted TSA every hour (different periods are possible, too) from GPS/Galileo time transfer receiver in Trusted TSA, and NMI. Time differences between Trusted TSA and NMI are computed by Control unit from common view timing data.

Common view timing data from NMI GPS time transfer receiver must be available on http- or ftp-server. This means that NMI has to be equipped with GPS time transfer receiver with integrated http-/ftp-server, or additional unit, which can provide data from receiver to the http-/ftp-server.

NTP time differences between Trusted TSA and NMI are read continuously by control unit from NTP system in Trusted TSA.

### 5.2. Time Synchronization Component ↔ TSU

The interface between Time Synchronization Component and the TSU depends on the chosen off-the-shelf TSU. The Time Synchronization Component must implement the interface used by the TSU. We propose to push the current time (and date) to the TSU on a regular basis with a frequency that will be fixed in WP3. The transmission of the timing information on request from TSU is also predicted.

### 5.3. TSU ↔ Archival Unit

When the TSU has issued a timestamp, it sends it also to the archive. In the other direction, the archival unit regularly sends its latest linking item to the TSU, such that the TSU can include it in the timestamps.

#### Timestamps to the archive

Whenever the TSU has created a new timestamp S, it is sent to the archival unit. The contents of the message is just S. The connection from the TSU to

the archival unit is TCP-like, guaranteeing the arrival of all sent messages in the correct order.

#### Linking items to timestamps

Periodically, the archival unit sends its last linking item to the TSU. The period corresponds to the granularity of time when comparing two timestamps based on their linking information. The contents of the message is the sequence number n of the last linking item, and the contents of that linking item Ln (a bit-string). The flow control has to ensure that the messages receive in order. However, it does not make sense to make sure that the TSU receives all messages – if the time to send the next message has arrived the attempts to send the previous message should end.

### 5.4. Time Synchronization Component ↔ Archival Unit

The Time Synchronization Component logs its internal events in the archival unit. The descriptions of these events are handled by the archive in the same way as the timestamps received from the TSU. The list of internal events to be logged may contain the failure of a time standard, the change of the used time standard (by the multiplexer), the download of common view timing data (including a cryptographic hash of that data), etc.

Every record to the digital archive must be additionally supplied by time - date information obtained directly from NMI - TSU interface (see Fig. 1). This information will be used for control uncertainties of issued Time Stamps. Transmission of time - date information can be done by:

- COM port;
- NTP protocol;
- IRIG-B code;
- PPS signals combined with IRIG-B code.

Application of COM port or NTP protocol technologies does not require additional hardware.

Implementation of IRIG-B code based technologies allow to achieve the one millisecond precision of timing information.

NTP technology is the optimal technology for time - date information transmission from NMI -TSU interface to the digital archive. In special cases other technologies can be implemented for that.

### 5.5. TSU ↔ Client

TSU receives time stamping requests from clients. These requests confirm to [1]. In particular, they contain the hash D of the time stamped document or signature. The timestamp T given to D also confirms to [1]. The timestamp T also contains the relevant linking information (n,L,,). It is added to timestamps in the following way.

[1] defines a TimeStampToken - the contents of a timestamp - as ContentInfo [3] whose field content has the type SignedData [3]. This data structure in turn has a field signerInfos which is a set of records of type SignerInfo. In [1] it is specified that for timestamps, this set must contain exactly one element - the signature and related info by the TSA. The records of type SignerInfo have an optional field

signedAttrs which, if it is present, is a set of records of type Attribute. A record of type Attribute has two fields - its type (an object identifier) and its content. The linking information is included in a timestamp as a signed attribute. An object identifier, as well as a content type will be defined in one of the deliverables for system architecture. This content type will include the sequence number n of the linking information, as well as that information L<sub>n</sub>, itself. The standards [1] and [6] do not prohibit the addition of such an attribute.

When a client receives such a timestamp it has to perform the checks listed in [1] and/or [3]. I.e. the inclusion of linking information does not make any extra checks by the client necessary at this point.

### 5.6. Archival Unit ↔ Client

The clients may query the archival unit for linking chains between two timestamps. The purpose of these queries may be to obtain the proof on the temporal ordering of these timestamps. The purpose may also be to audit the TSA, by asking for a linking chain between two timestamps that still have valid TSA signatures.

The query from the client to the archival unit contains two timestamps, T<sub>1</sub> and T<sub>2</sub>. If the archival unit and the TSU are located physically in the same place then the query also has to contain its type. The response by the archival unit contains the following information:

- a bit denoting whether T<sub>1</sub> or T<sub>2</sub> was earlier;
- a linking chain. It is a sequence of bit-strings (X<sub>1</sub>,...,X<sub>k</sub>) and a bit-string b<sub>1</sub>...b<sub>k</sub> of the same length.

Alternatively, the response by the archival unit may be an error message stating that it could not find a suitable linking chain.

If the client received a positive response then it verifies the linking chain in the way described in the use cases. Namely, it sets Y<sub>0</sub> equal to the timestamp which was denoted to be earlier and

$$Y_i = \begin{cases} Y_{i-1}, X_i & \text{if } b_i = 1 \\ X_i, Y_{i-1} & \text{if } b_i = 0 \end{cases}$$

computes Y<sub>1</sub>,...,Y<sub>k</sub> by

The client verifies that Y<sub>k</sub> equals the linking information in the timestamp which was denoted to be later. If not, the client does not accept the linking chain. If both T<sub>1</sub> and T<sub>2</sub> still have valid TSA signatures then the archival unit is under obligation to produce a valid linking chain. If it fails to do so, the client can lodge a complaint against the TSA, accusing it in cheating.

### 5.7. Control System ↔ anything else

The Control System is responsible for running the other parts of the time stamping server. Its duties, causing communication between it and the other parts of the system, include

- Monitoring, control and measuring characteristics of NMI-TSU interface.
- TSU functions monitoring and control;

- Installing and renewing of TSU certificates;
- Network components management by using SNMP protocol;
- Management of users and user rights;
- TSA service accounting
- Centralized data base administration;
- Backing up and restoring of archive data;
- Automated analysis of TSA system events (failures and other) and reacting upon them (for example, stopping the time stamping).

Concrete functions and realization of Control System depends on the hardware used in other TSA parts.

### 5.8. Main system ↔ Remote system in general

The connection between the possibly geographically separated systems must be secure. As a simple solution, we envision the creation of a virtual private network (VPN) connecting all sites; most probably an off-the-shelf VPN product can be used here. The choice of the VPN will be made in later, considering the bandwidth and latency of the secure network thus achieved, as well as the simplicity of key management.

### 5.9. Time Synchronization Component ↔ Remote Timing Unit

The synchronization between the components of time mark synchronization at the main system and at the remote system can be achieved through the transmission of 1pps signal over coaxial cable or glass fiber (for relatively short distances). Secure LAN connection for the information exchange (common view timing data) with Control Unit of Timing System is also required; this can be provided by the VPN mentioned above.

### 5.10. Archival Unit ↔ Archival Unit

To synchronize the linking chains, the archival units periodically send their last linking items to other archival units; the addresses of these units, as well as the periods are included in the configuration of the archival units. A message contains the sequence number n of the last linking item and the linking item L<sub>n</sub>, itself. A message also contains the name of the sending archival unit (although it probably does not make sense to cryptographically authenticate the sender). If the communicating archival units belong to the same TSA (i.e. one is at the main system while the other is at the remote system) then the messages are sent through the VPN tunnel set up between these two locations.

### 5.11. TSU ↔ Certification Authority

The standard [5] requires that the verification key corresponding to the signature key of the TSU is made available inside a public-key certificate issued by a Certification Authority (CA) with a certificate policy providing a sufficiently high level of security. The details of the communication depend on the technical and political details of the CA, but there at least have to be means to obtain a certificate for a new verification key (together with its addition in some public directory) and for prematurely revoking a verification key.

## 6. Organizational Requirements

The security of time stamping, i.e. the impossibility of back-dating is somewhat dependent on the secrecy of the key used to sign the timestamps. Hence we require that the key is treated accordingly to [5]. Fortunately, if something goes wrong here we can still use the archive of issued timestamps.

The TSA's policy also has to state the precision of times included in the timestamps. These requirements are also stated more precisely in [5].

The contents of the archive must be protected from modification; the TSA's policy must state how this is achieved. We will formulate the necessary level of protection in WP4. If the contents of the archive has been modified then this may be discovered by comparing the contents of this archive with the contents of archives of other TSA's.

The archive is also necessary for comparing the timestamps if the signatures cannot be used. Hence the archive must have high availability. TSA's policy must state how this is achieved. In particular, it must state how the archive remains accessible if the TSA stops operating.

## 7. References

[1] Adams, C. Cain, P. Pinkas, D. and Zuccherato, R. "*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*", IETF RFC 3161, August 2001.

[2] Ekstrom, C. and Koppang, P. "*Three-Cornered Hats and Degrees of Freedom*", Proceedings of the 33rd Annual Precise Time and Time Interval (PTTI) Systems and Applications Meeting, November 2001, pp. 425-430.

[3] Housley, R. "*Cryptographic Message Syntax*", IETF RFC 3852, July 2004.

[4] Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats. European Telecommunications Standards Institute Technical Specification 101 733 v.1.5.1, December 2003.

[5] Policy requirements for time-stamping authorities. European Telecommunications Standards Institute Technical Specification 102 023 (ETSI TS 102 023), v.1.2.1, January 2003.

[6] Time stamping profile. European Telecommunications Standards Institute Technical Specification 101 861 (ETSI TS 101 861), v.1.3.1, January 2006.

Copyright © 2008 by the International Business Information Management Association (IBIMA). All rights reserved. Authors retain copyright for their manuscripts and provide this journal with a publication permission agreement as a part of IBIMA copyright agreement. IBIMA may not necessarily agree with the content of the manuscript. The content and proofreading of this manuscript as well as and any errors are the sole responsibility of its author(s). No part or all of this work should be copied or reproduced in digital, hard, or any other format for commercial use without written permission. To purchase reprints of this article please e-mail: [admin@ibima.org](mailto:admin@ibima.org).