Network Working Group
Request for Comments: 3628
Category: Informational

D. Pinkas
Bull
N. Pope
J. Ross
Security & Standards

November 2003

Policy Requirements for Time-Stamping Authorities (TSAs)

Status of this Memo

Copyright Notice

Abstract

This document defines requirements for a baseline time-stamp policy for Time-Stamping Authorities (TSAs) issuing time-stamp tokens, supported by public key certificates, with an accuracy of one second or better. A TSA may define its own policy which enhances the policy defined in this document. Such a policy shall incorporate or further constrain the requirements identified in this document.

Table of Contents

1. Introduction

The contents of this Informational RFC is technically equivalent to ETSI TS 102 023 V 1.2.1 (2002-06) [TS 102023]. The ETSI TS is under the ETSI Copyright (C). Individual copies of this ETSI deliverable can be downloaded from http://www.etsi.org

In creating reliable and manageable digital evidence it is necessary to have an agreed upon method of associating time data to transaction so that they might be compared to each other at a later time. The quality of this evidence is based on creating and managing the data structure that represent the events and the quality of the parametric data points that anchor them to the real world. In this instance this being the time data and how it was applied.

A typical transaction is a digitally signed document, where it is necessary to prove that the digital signature from the signer was applied when the signer's certificate was valid.

A timestamp or a time mark (which is an audit record kept in a secure audit trail from a trusted third party) applied to a digital signature value proves that the digital signature was created before the date included in the time-stamp or time mark.

To prove the digital signature was generated while the signer's certificate was valid, the digital signature must be verified and the following conditions satisfied:

1. the time-stamp (or time mark) was applied before the end of the validity period of the signer's certificate,

2. the time-stamp (or time mark) was applied either while the signer's certificate was not revoked or before the revocation date of the certificate.

Thus a time-stamp (or time mark) applied in this manner proves that the digital signature was created while the signer's certificate was valid. This concept proves the validity of a digital signature over the whole of any certificate chain.

Policy requirements to cover that case is the primary reason of this document. However, it should be observed that these policy requirements can be used to address other needs.

The electronic time stamp is gaining interest from the business sector as an important component of electronic signatures. It is also featured by the ETSI Electronic Signature Format standard [TS 101733] or Electronic Signature Formats for long term electronic signatures [RFC 3126], built upon the Time-Stamp Protocol [RFC 3161]. Agreed minimum security and quality requirements are necessary in order to ensure trustworthy validation of long-term electronic signatures.

The European Directive 1999/93/EC [Dir 99/93/EC] defines certification service provider as "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures". One example of a certification-service-provider is a Time-Stamping Authority.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC 2119].

2. Overview

These policy requirements are aimed at time-stamping services used in support of qualified electronic signatures (i.e., in line with article 5.1 of the European Directive on a community framework for electronic signatures) but may be applied to any application requiring to prove that a datum existed before a particular time.

These policy requirements are based on the use of public key cryptography, public key certificates and reliable time sources. The present document may be used by independent bodies as the basis for confirming that a TSA may be trusted for providing time-stamping services.

This document addresses requirements for synchronizing TSAs issuing time-stamp tokens with Coordinated universal time (UTC) and digitally signed by TSUs.

Subscriber and relying parties should consult the TSA’s practice statement to obtain further details of precisely how this time-stamp policy is implemented by the particular TSA (e.g., protocols used in providing this service).

This document does not specify:

- protocols used to access the TSUs;

NOTE 1: A time-stamping protocol is defined in RFC 3161 [RFC 3161] and profiled in TS 101 861 [TS 101861].

- how the requirements identified herein may be assessed by an independent body;
- requirements for information to be made available to such independent bodies;
- requirements on such independent bodies.

NOTE 2: See CEN Workshop Agreement 14172 "EESSI Conformity Assessment Guidance" [CWA 14172].

3. Definitions and Abbreviations

3.1. Definitions

For the purposes of the present document, the following terms and definitions apply:

NOTE: Where a definition is copied from a referenced document this is indicated by inclusion of the reference identifier number at the end of the definition.

relying party: recipient of a time-stamp token who relies on that time-stamp token.

subscriber: entity requiring the services provided by a TSA and which has explicitly or implicitly agreed to its terms and conditions.

time-stamp token: data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.

time-stamping authority: authority which issues time-stamp tokens.

TSA Disclosure statement: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements.

TSA practice statement: statement of the practices that a TSA employs in issuing time-stamp tokens.

TSA system: composition of IT products and components organized to support the provision of time-stamping services.

time-stamp policy: named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements.

time-stamping unit: set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time.

Coordinated Universal Time (UTC): Time scale based on the second as defined in ITU-R Recommendation TF.460-5 [TF.460-5].

NOTE: For most practical purposes UTC is equivalent to mean solar time at the prime meridian. More specifically, UTC is a compromise between the highly stable atomic time (Temps Atomique International - TAI) and solar time derived from the irregular Earth rotation (related to the Greenwich mean sidereal time (GMST) by a conventional relationship). (See annex A for more details).

UTC(k): Time-scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach plus or minus 100 ns. (See ITU-R Recommendation TF.536-1 [TF.536-1]).

NOTE: A list of UTC(k) laboratories is given in section 1 of Circular T disseminated by BIPM and available from the BIPM website (http://www.bipm.org/).

3.2. Abbreviations

For the purposes of the present document, the following abbreviations apply:

TSA Time-Stamping Authority
TSU Time-Stamping Unit
TST Time-Stamp Token
UTC Coordinated Universal Time

4. General Concepts

4.1. Time-Stamping Services

The provision of time-stamping services is broken down into the following component services for the purposes of classifying requirements:

- Time-stamping provision: This service component generates time-stamp tokens.

- Time-stamping management: The service component that monitors and controls the operation of the time-stamping services to ensure that the service is provided as specified by the TSA. This service component is responsibile for the installation and de-installation of the time-stamping provision service. For example, time-stamping management ensures that the clock used for time-stamping is correctly synchronized with UTC.

This subdivision of services is only for the purposes of clarifying the requirements specified in the current document and places no restrictions on any subdivision of an implementation of time-stamping services.

4.2. Time-Stamping Authority

The authority to issue time-stamp tokens, trusted by the users of the time-stamping services, i.e., subscribers and relying parties, is called the Time-Stamping Authority (TSA). TSA has overall responsibility for time-stamping services identified in clause 4.1. The TSA has responsibility for the operation of one or more TSU's which creates and signs on behalf of the TSA. The TSA responsible for issuing a time-stamp token is identifiable (see 7.3.1 h).

The TSA may use other parties to provide parts of the Time-Stamping Services. However, the TSA always maintains overall responsibility and ensures that the policy requirements identified in the present document are met. For example, a TSA may sub-contract all the component services, including the services which generate time-stamp tokens using the TSU's keys. However, the private key or keys used to generate the time-stamp tokens belong to the TSA which maintains overall responsibility for meeting the requirements in this document.

A TSA may operate several identifiable time-stamping units. Each unit has a different key. See Annex B for possible implementations.

A TSA is a certification-service-provider, as defined in the EU Directive on Electronic Signatures (see article 2(11)), which issues time-stamp tokens.

4.3. Subscriber

The subscriber may be an organization comprising several end-users or an individual end-user.

When the subscriber is an organization, some of the obligations that apply to that organization will have to apply as well to the end-users. In any case the organization will be held responsible if the

obligations from the end-users are not correctly fulfilled and therefore the organization is expected to suitably inform its end users.

When the subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

4.4. Time-Stamp Policy and TSA Practice Statement

This section explains the relative roles of Time-stamp policy and TSA practice statement. It places no restriction on the form of a time-stamp policy or practice statement specification.

4.4.1. Purpose

In general, the time-stamp policy states "what is to be adhered to," while a TSA practice statement states "how it is adhered to", i.e., the processes it will use in creating time-stamps and maintaining the accuracy of its clock. The relationship between the time-stamp policy and TSA practice statement is similar in nature to the relationship of other business policies which state the requirements of the business, while operational units define the practices and procedures of how these policies are to be carried out.

The present document specifies a time-stamp policy to meet general requirements for trusted time-stamping services. TSAs specify in TSA practice statements how these requirements are met.

4.4.2. Level of Specificity

The TSA practice statement is more specific than a time-stamp policy. A TSA practice statement is a more detailed description of the terms and conditions as well as business and operational practices of a TSA in issuing and otherwise managing time-stamping services. The TSA practice statement of a TSA enforces the rules established by a time-stamp policy. A TSA practice statement defines how a specific TSA meets the technical, organizational and procedural requirements identified in a time-stamp policy.

NOTE: Even lower-level internal documentation may be appropriate for a TSA detailing the specific procedures necessary to complete the practices identified in the TSA practice statement.

4.4.3. Approach

The approach of a time-stamp policy is significantly different from a TSA practice statement. A time-stamp policy is defined independently of the specific details of the specific operating environment of a

TSA, whereas a TSA practice statement is tailored to the organizational structure, operating procedures, facilities, and computing environment of a TSA. A time-stamp policy may be defined by the user of times-stamp services, whereas the TSA practice statement is always defined by the provider.

5. Time-Stamp Policies

5.1. Overview

A time-stamp policy is a "named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements" (see clauses 3.1 and 4.4).

The present document defines requirements for a baseline time-stamp policy for TSAs issuing time-stamp tokens, supported by public key certificates, with an accuracy of 1 second or better.

NOTE 1: Without additional measures the relying party may not be able to ensure the validity of a time-stamp token beyond the end of the validity period of the supporting certificate. See Annex C on verification of the validity of a time-stamp token beyond the validity period of the TSU's certificate.

A TSA may define its own policy which enhances the policy defined in this document. Such a policy shall incorporate or further constrain the requirements identified in this document.

If an accuracy of better than 1 second is provided by a TSA and if all the TSUs have that same characteristics, then the accuracy shall be indicated in the TSA's disclosure statement (see section 7.1.2) that each time-stamp token is issued with an accuracy of better than 1 second.

NOTE 2: It is required that a time-stamp token includes an identifier for the applicable policy (see section 7.3.1).

5.2. Identification

The object-identifier [X.208] of the baseline time-stamp policy is: itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1)

In the TSA disclosure statement made available to subscribers and relying parties, a TSA shall also include the identifier for the time-stamp policy to indicate its conformance.

5.3. User Community and Applicability

This policy is aimed at meeting the requirements of time-stamping qualified electronic signatures (see European Directive on Electronic Signatures) for long term validity (e.g., as defined in TS 101 733 [TS 101733]), but is generally applicable to any requirement for an equivalent quality.

This policy may be used for public time-stamping services or time-stamping services used within a closed community.

5.4. Conformance

The TSA shall use the identifier for the time-stamp policy in time-stamp tokens as given in section 5.2, or define its own time-stamp policy that incorporates or further constrains the requirements identified in the present document:

a) if the TSA claims conformance to the identified time-stamp policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance; or

b) if the TSA has been assessed to conform to the identified time-stamp policy by an independent party.

A conformant TSA must demonstrate that:

a) it meets its obligations as defined in section 6.1;
b) it has implemented controls which meet the requirements specified in section 7.

6. Obligations and Liability

6.1. TSA Obligations

6.1.1. General

The TSA shall ensure that all requirements on TSA, as detailed in section 7, are implemented as applicable to the selected trusted time-stamp policy.

The TSA shall ensure conformance with the procedures prescribed in this policy, even when the TSA functionality is undertaken by sub-contractors.

The TSA shall also ensure adherence to any additional obligations indicated in the time-stamp either directly or incorporated by reference.

The TSA shall provide all its time-stamping services consistent with its practice statement.

6.1.2. TSA Obligations Towards Subscribers

The TSA shall meet its claims as given in its terms and conditions including the availability and accuracy of its service.

6.2. Subscriber Obligations

The current document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the TSA's terms and condition.

NOTE: It is advisable that, when obtaining a time-stamp token, the subscriber verifies that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp token has not been compromised.

6.3. Relying Party Obligations

The terms and conditions made available to relying parties (see section 7.1.2) shall include an obligation on the relying party that, when relying on a time-stamp token, it shall:

a) verify that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification;

   NOTE: During the TSU's certificate validity period, the validity of the signing key can be checked using current revocation status for the TSU's certificate. If the time of verification exceeds the end of the validity period of the corresponding certificate, see annex C for guidance.

b) take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy;

c) take into account any other precautions prescribed in agreements or elsewhere.

6.4. Liability

The present document does not specify any requirement on liability. In particular, it should be noticed that a TSA may disclaim or limit any liability unless otherwise stipulated by the applicable law.

7. Requirements on TSA Practices

The TSA shall implement the controls that meet the following requirements.

These policy requirements are not meant to imply any restrictions on charging for TSA services.

The requirements are indicated in terms of the security objectives, followed by more specific requirements for controls to meet those objectives where it is necessary to provide confidence that those objective will be met.

> NOTE: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a TSA may employ in issuing time-stamp tokens. In the case of section 7.4 (TSA management and operation), a reference is made to a source of more detailed control requirements. Due to these factors the specificity of the requirements given under a given topic may vary.

The provision of a time-stamp token in response to a request is at the discretion of the TSA depending on any service level agreements with the subscriber.

7.1. Practice and Disclosure Statements

7.1.1. TSA Practice Statement

The TSA shall ensure that it demonstrates the reliability necessary for providing time-stamping services.

In particular:

a) The TSA shall have a risk assessment carried out in order to evaluate business assets and threats to those assets in order to determine the necessary security controls and operational procedures.

b) The TSA shall have a statement of the practices and procedures used to address all the requirements identified in this time-stamp policy.

> NOTE 1: This policy makes no requirement as to the structure of the TSA practice statement.

c) The TSA's practice statement shall identify the obligations of all external organizations supporting the TSA services including the applicable policies and practices.

d) The TSA shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary, to assess conformance to the time-stamp policy.

NOTE 2: The TSA is not generally required to make all the details of its practices public.

e) The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services as specified in section 7.1.2.

f) The TSA shall have a high level management body with final authority for approving the TSA practice statement.

g) The senior management of the TSA shall ensure that the practices are properly implemented.

h) The TSA shall define a review process for the practices including responsibilities for maintaining the TSA practice statement.

i) The TSA shall give due notice of changes it intends to make in its practice statement and shall, following approval as in (f) above, make the revised TSA practice statement immediately available as required under (d) above.

7.1.2. TSA Disclosure Statement

The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services. This statement shall at least specify for each time-stamp policy supported by the TSA:

a) The TSA contact information.

b) The time-stamp policy being applied.

c) At least one hashing algorithm which may be used to represent the datum being time-stamped. (No hash algorithm is mandated).

d) The expected life-time of the signature used to sign the time-stamp token (depends on the hashing algorithm being used, the signature algorithm being used and the private key length).

e) The accuracy of the time in the time-stamp tokens with respect to UTC.

f) Any limitations on the use of the time-stamping service.

g) The subscriber's obligations as defined in section 6.2, if any.

h) The relying party's obligations as defined in section 6.3.

i) Information on how to verify the time-stamp token such that the relying party is considered to "reasonably rely" on the time-stamp token (see section 6.3) and any possible limitations on the validity period.

j) The period of time during which TSA event logs (see section 7.4.10) are retained.

k) The applicable legal system, including any claim to meet the requirements on time-stamping services under national law.

l) Limitations of liability.

m) Procedures for complaints and dispute settlement.

n) If the TSA has been assessed to be conformant with the identified time-stamp policy, and if so by which independent body.

NOTE 1: It is also recommended that the TSA includes in its time-stamping disclosure statement availability of its service, for example the expected mean time between failure of the time-stamping service, the mean time to recovery following a failure, and provisions made for disaster recovery including back-up services;

This information shall be available through a durable means of communication. This information shall be available in a readily understandable language. It may be transmitted electronically.

NOTE 2: A model TSA disclosure statement which may be used as the basis of such a communication is given in annex D. Alternatively this may be provided as part of a subscriber / relying party agreement. These TSA disclosure statements may be included in a TSA practice statement provided that they are conspicuous to the reader.

7.2. Key Management Life Cycle

7.2.1. TSA Key Generation

The TSA shall ensure that any cryptographic keys are generated in under controlled circumstances.

In particular:

a) The generation of the TSU's signing key(s) shall be undertaken in a physically secured environment (see section 7.4.4) by personnel in trusted roles (see section 7.4.3) under, at least, dual control. The personnel authorized to carry out this function shall be limited to those requiring to do so under the TSA's practices.

b) The generation of the TSU's signing key(s) shall be carried out within a cryptographic module(s) which either:

   - meets the requirements identified in FIPS 140-1 [FIPS 140-1] level 3 or higher, or

   - meets the requirements identified in CEN Workshop Agreement 14167-2 [CWA 14167-2], or

   - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO 15408 [ISO 15408], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the current document, based on a risk analysis and taking into account physical and other non-technical security measures.

c) The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamp tokens key shall be recognized by any national supervisory body, or in accordance with existing current state of art, as being fit for the purposes of time-stamp tokens as issued by the TSA.

7.2.2. TSU Private Key Protection

The TSA shall ensure that TSU private keys remain confidential and maintain their integrity.

In particular:

a) The TSU private signing key shall be held and used within a cryptographic module which:

- meets the requirements identified in FIPS 140-1 [FIPS 140-1] level 3 or higher; or

- meets the requirements identified in CEN Workshop Agreement 14167-2 [CWA 14167-2]; or

- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO 15408 [ISO 15408], or equivalent security criteria. This shall be a security target or protection profile which meets the requirements of the current document, based on a risk analysis and taking into account physical and other non-technical security measures.

NOTE: Backup of TSU private keys is deprecated in order to minimize risk of key compromise.

b) If TSU private keys are backed up, they shall be copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. (see section 7.4.4). The personnel authorized to carry out this function shall be limited to those requiring to do so under the TSA's practices.

c) Any backup copies of the TSU private signing keys shall be protected to ensure its confidentiality by the cryptographic module before being stored outside that device.

7.2.3. TSU Public Key Distribution

The TSA shall ensure that the integrity and authenticity of the TSU signature verification (public) keys and any associated parameters are maintained during its distribution to relying parties.

In particular:

a) TSU signature verification (public) keys shall be made available to relying parties in a public key certificate.

NOTE: For example, TSU's certificates may be issued by a certification authority operated by the same organization as the TSA, or issued by another authority.

b) The TSU's signature verification (public) key certificate shall be issued by a certification authority operating under a certificate policy which provides a level of security equivalent to, or higher than, this time-stamping policy.

7.2.4. Rekeying TSU's Key

The life-time of TSU's certificate shall be not longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose (see section 7.2.1c)).

NOTE 1: The following additional considerations apply when limiting that lifetime:

- Section 7.4.10 requires that records concerning time-stamping services shall be held for a period of time,as appropriate, for at least 1 year after the expiration of the validity of the TSU's signing keys. The longer the validity period of the TSU certificates will be, the longer the size of the records to be kept will be.

- Should a TSU private key be compromised, then the longer the life-time, the more affected time-stamp tokens there will be.

NOTE 2: TSU key compromise does not only depend on the characteristics of the cryptographic module being used but also on the procedures being used at system initialization and key export (when that function is supported).

7.2.5. End of TSU Key Life Cycle

The TSA shall ensure that TSU private signing keys are not used beyond the end of their life cycle.

In particular:

a) Operational or technical procedures shall be in place to ensure that a new key is put in place when a TSU's key expires.

b) The TSU private signing keys, or any key part, including any copies shall be destroyed such that the private keys cannot be retrieved.

c) The TST generation system SHALL reject any attempt to issue TSTs if the signing private key has expired.

7.2.6. Life Cycle Management of the Cryptographic Module used to Sign Time-Stamps

The TSA shall ensure the security of cryptographic hardware throughout its lifecycle.

In particular the TSA shall ensure that:

a) Time-stamp token signing cryptographic hardware is not tampered with during shipment;

b) Time-stamp token signing cryptographic hardware is not tampered with while stored;

c) Installation, activation and duplication of TSU's signing keys in cryptographic hardware shall be done only by personnel in trusted roles using, at least, dual control in a physically secured environment. (see section 7.4.4);

d) Time-stamp token signing cryptographic hardware is functioning correctly; and

e) TSU private signing keys stored on TSU cryptographic module are erased upon device retirement.

7.3. Time-Stamping

7.3.1. Time-Stamp Token

The TSA shall ensure that time-stamp tokens are issued securely and include the correct time.

In particular:

a) The time-stamp token shall include an identifier for the time-stamp policy;

b) Each time-stamp token shall have a unique identifier;

c) The time values the TSU uses in the time-stamp token shall be traceable to at least one of the real time values distributed by a UTC(k) laboratory.

NOTE 1: The Bureau International des Poids et Mesures (BIPM) computes UTC on the basis of its local representations UTC(k) from a large ensemble of atomic clocks in national metrology institutes and national astronomical observatories round the world. The BIPM disseminates UTC through its monthly Circular T [list 1]. This is available on the BIPM website (www.bipm.org) and it officially identifies all those institutes having recognized UTC(k) time scales.

d) The time included in the time-stamp token shall be synchronized with UTC within the accuracy defined in this policy and, if present, within the accuracy defined in the time-stamp token itself;

e) If the time-stamp provider's clock is detected (see section 7.3.2c)) as being out of the stated accuracy (see section 7.1.2e)) then time-stamp tokens shall not be issued.

f) The time-stamp token shall include a representation (e.g., hash value) of the datum being time-stamped as provided by the requestor;

g) The time-stamp token shall be signed using a key generated exclusively for this purpose.

NOTE 2: A protocol for a time-stamp token is defined in RFC 3631 and profiled in TS 101 861 [TS 101861].

NOTE 3: In the case of a number of requests at approximately the same time, the ordering of the time within the accuracy of the TSU clock is not mandated.

h) The time-stamp token shall include:

- where applicable, an identifier for the country in which the TSA is established;

- an identifier for the TSA;

- an identifier for the unit which issues the time-stamps.

7.3.2. Clock Synchronization with UTC

The TSA shall ensure that its clock is synchronized with UTC within the declared accuracy.

In particular:

a) The calibration of the TSU clocks shall be maintained such that the clocks shall not be expected to drift outside the declared accuracy.

b) The TSU clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration.

NOTE 1: Threats may include tampering by unauthorized personnel, radio or electrical shocks.

c) The TSA shall ensure that, if the time that would be indicated in a time-stamp token drifts or jumps out of synchronization with UTC, this will be detected (see also 7.3.1e)).

NOTE 2: Relying parties are required to be informed of such events (see section 7.4.8).

d) The TSA shall ensure that clock synchronization is maintained when a leap second occurs as notified by the appropriate body. The change to take account of the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record shall be maintained of the exact time (within the declared accuracy) when this change occurred. See annex A for more details.

NOTE 3: A leap second is an adjustment to UTC by skipping or adding an extra second on the last second of a UTC month. First preference is given to the end of December and June, and second preference is given to the end of March and September.

7.4. TSA Management and Operation

7.4.1. Security Management

The TSA shall ensure that the administrative and management procedures applied are adequate and correspond to recognized best practice.

In particular:

TSA General

a) The TSA shall retain responsibility for all aspects of the provision of time-stamping services within the scope of this time-stamp policy, whether or not functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the TSA and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the TSA. The TSA shall retain responsibility for the disclosure of relevant practices of all parties.

b) The TSA management shall provide direction on information security through a suitable high level steering forum that is responsible for defining the TSA's information security policy. The TSA shall ensure publication and communication of this policy to all employees who are impacted by it.

c) The information security infrastructure necessary to manage the security within the TSA shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the TSA management forum.

NOTE 1: See ISO/IEC 17799 [ISO 17799] for guidance on information security management including information security infrastructure, management information security forum and information security policies.

d) The security controls and operating procedures for TSA facilities, systems and information assets providing the time-stamping services shall be documented, implemented and maintained.

NOTE 2: The present documentation (commonly called a system security policy or manual) should identify all relevant targets, objects and potential threats related to the services provided and the safeguards required to avoid or limit the effects of those threats, consistent with the Risk Assessment required under section 7.1.1a). It should describe the rules, directives and procedures regarding how the specified services and the associated security assurance are granted in addition to stating policy on incidents and disasters.

e) TSA shall ensure that the security of information is maintained when the responsibility for TSA functions has been outsourced to another organization or entity.

7.4.2. Asset Classification and Management

The TSA shall ensure that its information and other assets receive an appropriate level of protection.

In particular:

- The TSA shall maintain an inventory of all assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

7.4.3. Personnel Security

The TSA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the TSA's operations.

In particular (TSA general):

a) The TSA shall employ personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.

   NOTE 1: TSA personnel should be able to fulfill the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two.

   NOTE 2: Personnel employed by a TSA include individual personnel contractually engaged in performing functions in support of the TSA's time-stamping services. Personnel who may be involved in monitoring the TSA services need not be TSA personnel.

b) Security roles and responsibilities, as specified in the TSA's security policy, shall be documented in job descriptions. Trusted roles, on which the security of the TSA's operation is dependent, shall be clearly identified.

c) TSA personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Where appropriate, these shall differentiate between general functions and TSA specific functions. These should include skills and experience requirements.

d) Personnel shall exercise administrative and management procedures and processes that are in line with the TSA's information security management procedures (see section 7.4.1).

   NOTE 3: See ISO/IEC 17799 [ISO 17799] for guidance.

   The following additional controls shall be applied to time-stamping management:

e) Managerial personnel shall be employed who possess:

   - knowledge of time-stamping technology; and
   - knowledge of digital signature technology; and

- knowledge of mechanisms for calibration or synchronization the TSU clocks with UTC; and
- familiarity with security procedures for personnel with security responsibilities; and
- experience with information security and risk assessment.

f) All TSA personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSA operations.

g) Trusted roles include roles that involve the following responsibilities:

- Security Officers: Overall responsibility for administering the implementation of the security practices.

- System Administrators: Authorized to install, configure and maintain the TSA trustworthy systems for time-stamping management.

- System Operators: Responsible for operating the TSA trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery.

- System Auditors: Authorized to view archives and audit logs of the TSA trustworthy systems.

h) TSA personnel shall be formally appointed to trusted roles by senior management responsible for security.

i) The TSA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offense which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed.

NOTE 4: In some countries it may not be possible for TSA to obtain information on past convictions without the collaboration of the candidate employee.

7.4.4. Physical and Environmental Security

The TSA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized.

In particular (general):

a) For both the time-stamping provision and the time-stamping management:

- physical access to facilities concerned with time-stamping services shall be limited to properly authorized individuals;
- controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities; and
- controls shall be implemented to avoid compromise or theft of information and information processing facilities.

b) Access controls shall be applied to the cryptographic module to meet the requirements of security of cryptographic modules as identified in clauses 7.2.1 and 7.2.2.

c) The following additional controls shall be applied to time-stamping management:

- The time-stamping management facilities shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

- Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e., physical barriers) around the time-stamping management. Any parts of the premises shared with other organizations shall be outside this perimeter.

- Physical and environmental security controls shall be implemented to protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The TSA's physical and environmental security policy for systems concerned with time-stamping management shall address as a minimum the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g., power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

- Controls shall be implemented to protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization.

NOTE 1: See ISO/IEC 17799 [ISO 17799] for guidance on physical and environmental security.

NOTE 2: Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.

7.4.5. Operations Management

The TSA shall ensure that the TSA system components are secure and correctly operated, with minimal risk of failure:

In particular (general):

a) The integrity of TSA system components and information shall be protected against viruses, malicious and unauthorized software.

b) Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions shall be minimized.

c) Media used within the TSA trustworthy systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence.

NOTE 1: Every member of personnel with management responsibilities is responsible for planning and effectively implementing the time-stamp policy and associated practices as documented in the TSA practice statement.

d) Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of time-stamping services.

Media handling and security

e) All media shall be handled securely in accordance with requirements of the information classification scheme (see section 7.4.2). Media containing sensitive data shall be securely disposed of when no longer required.

System Planning

f) Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Incident reporting and response

g) The TSA shall act in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident.

The following additional controls shall be applied to time-stamping management:

Operations procedures and responsibilities

h) TSA security operations shall be separated from other operations.

NOTE 2: TSA security operations' responsibilities include:

- operational procedures and responsibilities;
- secure systems planning and acceptance;
- protection from malicious software;
- housekeeping;
- network management;
- active monitoring of audit journals, event analysis and follow-up;
- media handling and security;
- data and software exchange.

These operations shall be managed by TSA trusted personnel, but, may actually be performed by, non-specialist, operational personnel (under supervision), as defined within the appropriate security policy, and, roles and responsibility documents.

7.4.6. System Access Management

The TSA shall ensure that TSA system access is limited to properly authorized individuals.

In particular (general):

a) Controls (e.g., firewalls) shall be implemented to protect the TSA's internal network domains from unauthorized access including access by subscribers and third parties.

NOTE 1: Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSA.

b) The TSA shall ensure effective administration of user (this includes operators, administrators and auditors) access to maintain system security, including user account management, auditing and timely modification or removal of access.

c) The TSA shall ensure that access to information and application system functions is restricted in accordance with the access control policy and that the TSA system provides sufficient computer security controls for the separation of trusted roles identified in TSA's practices, including the separation of security administrator and operation functions. Particularly, use of system utility programs is restricted and tightly controlled.

d) TSA personnel shall be properly identified and authenticated before using critical applications related to time-stamping.

e) TSA personnel shall be accountable for their activities, for example by retaining event logs (see section 7.4.10).

The following additional controls shall be applied to time-stamping management:

f) The TSA shall ensure that local network components (e.g., routers) are kept in a physically secure environment and that their configurations are periodically audited for compliance with the requirements specified by the TSA.

g) Continuous monitoring and alarm facilities shall be provided to enable the TSA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

NOTE 2: This may use, for example, an intrusion detection system, access control monitoring and alarm facilities.

7.4.7. Trustworthy Systems Deployment and Maintenance

The TSA shall use trustworthy systems and products that are protected against modification.

NOTE: The risk analysis carried out on the TSA's services (see section 7.1.1) should identify its critical services requiring trustworthy systems and the levels of assurance required.

In particular:

a) An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the TSA or on behalf of the TSA to ensure that security is built into IT systems.

b) Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software.

7.4.8. Compromise of TSA Services

The TSA shall ensure in the case of events which affect the security of the TSA's services, including compromise of TSU's private signing keys or detected loss of calibration, that relevant information is made available to subscribers and relying parties.

In particular:

a) The TSA's disaster recovery plan shall address the compromise or suspected compromise of TSU's private signing keys or loss of calibration of a TSU clock, which may have affected time-stamp tokens which have been issued.

b) In the case of a compromise, or suspected compromise or loss of calibration the TSA shall make available to all subscribers and relying parties a description of compromise that occurred.

c) In the case of compromise to a TSU's operation (e.g., TSU key compromise), suspected compromise or loss of calibration the TSU shall not issue time-stamp tokens until steps are taken to recover from the compromise

d) In case of major compromise of the TSA's operation or loss of calibration, wherever possible, the TSA shall make available to all subscribers and relying parties information which may be used to identify the time-stamp tokens which may have been affected, unless this breaches the privacy of the TSAs users or the security of the TSA services.

NOTE: In case the private key does become compromised, an audit trail of all tokens generated by the TSA may provide a means to discriminate between genuine and false backdated tokens. Two time-stamp tokens from two different TSAs may be another way to address this issue.

7.4.9. TSA Termination

The TSA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the TSA's time-stamping services, and in particular ensure continued maintenance of information required to verify the correctness of time-stamp tokens.

In particular:

a) Before the TSA terminates its time-stamping services the following procedures shall be executed as a minimum:

   - the TSA shall make available to all subscribers and relying parties information concerning its termination;

   - TSA shall terminate authorization of all subcontractors to act on behalf of the TSA in carrying out any functions relating to the process of issuing time-stamp tokens;

   - the TSA shall transfer obligations to a reliable party for maintaining event log and audit archives (see section 7.4.10) necessary to demonstrate the correct operation of the TSA for a reasonable period;

   - the TSA shall maintain or transfer to a reliable party its obligations to make available its public key or its certificates to relying parties for a reasonable period;

   - TSU private keys, including backup copies, shall be destroyed in a manner such that the private keys cannot be retrieved.

b) The TSA shall have an arrangement to cover the costs to fulfill these minimum requirements in case the TSA becomes bankrupt or for other reasons is unable to cover the costs by itself.

c) The TSA shall state in its practices the provisions made for termination of service. This shall include:

   - notification of affected entities;
   - transferring the TSA obligations to other parties.

d) The TSA shall take steps to have the TSU's certificates revoked.

7.4.10. Compliance with Legal Requirements

The TSA shall ensure compliance with legal requirements.

In particular:

a) The TSA shall ensure that the requirements of the European data protection Directive [Dir 95/46/EC], as implemented through national legislation, are met.

b) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

c) The information contributed by users to the TSA shall be completely protected from disclosure unless with their agreement or by court order or other legal requirement.

7.4.11. Recording of Information Concerning Operation of Time-Stamping Services

The TSA shall ensure that all relevant information concerning the operation of time-stamping services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings.

In particular:

General

a) The specific events and data to be logged shall be documented by the TSA.

b) The confidentiality and integrity of current and archived records concerning operation of time-stamping services shall be maintained.

c) Records concerning the operation of time-stamping services shall be completely and confidentially archived in accordance with disclosed business practices.

d) Records concerning the operation of time-stamping services shall be made available if required for the purposes of providing evidence of the correct operation of the time-stamping services for the purpose of legal proceedings.

e) The precise time of significant TSA environmental, key management and clock synchronization events shall be recorded.

f) Records concerning time-stamping services shall be held for a period of time after the expiration of the validity of the TSU's

signing keys as appropriate for providing necessary legal evidence and as notified in the TSA disclosure statement (see section 7.1.2).

g) The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

NOTE: This may be achieved, for example, through the use of write-only media, a record of each removable media used and the use of off-site backup.

h) Any information recorded about subscribers shall be kept confidential except as where agreement is obtained from the subscriber for its wider publication.

TSU key management

i) Records concerning all events relating to the life-cycle of TSU keys shall be logged.

j) Records concerning all events relating to the life-cycle of TSU certificates (if appropriate) shall be logged.

Clock Synchronization

k) Records concerning all events relating to synchronization of a TSU's clock to UTC shall be logged. This shall include information concerning normal re-calibration or synchronization of clocks use in time-stamping.

l) Records concerning all events relating to detection of loss of synchronization shall be logged.

7.5. Organizational

The TSA shall ensure that its organization is reliable.

In particular that:

a) Policies and procedures under which the TSA operates shall be non-discriminatory.

b) The TSA shall make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSA disclosure statement.

c) The TSA is a legal entity according to national law.

d) The TSA has a system or systems for quality and information security management appropriate for the time-stamping services it is providing.

e) The TSA has adequate arrangements to cover liabilities arising from its operations and/or activities.

f) It has the financial stability and resources required to operate in conformity with this policy.

NOTE 1: This includes requirements for TSA termination identified in section 7.4.9.

g) It employs a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide time-stamping services.

NOTE 2: Personnel employed by a TSA include individual personnel contractually engaged in performing functions in support of the TSA's time-stamping services. Personnel who may be involved only in monitoring the TSA services need not be TSA personnel.

h) It has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of the time-stamping services or any other related matters.

i) It has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

8. Security Considerations

When verifying time-stamp tokens it is necessary for the verifier to ensure that the TSU certificate is trusted and not revoked. This means that the security is dependent upon the security of the CA that has issued the TSU certificate for both issuing the certificate and providing accurate revocation status information for that certificate.

When a time-stamp is verified as valid at a given point of time, this does not mean that it will necessarily remain valid later on. Every time, a time-stamp token is verified during the validity period of the TSU certificate, it must be verified again against the current revocation status information, since in case of compromise of a TSU

private key, all the time-stamp tokens generated by that TSU become invalid. Annex C provides guidance about the long term verification of time-stamp tokens.

In applying time-stamping to applications, consideration also needs to be given to the security of the application. In particular, when applying time-stamps it is necessary to ensure that the integrity of data is maintained before the time-stamp is applied. The requester ought to really make sure that the hash value included in the time-stamp token matches with the hash of the data.

9. Acknowledgments

The development of this document was supported by ETSI and the European Commission. Special thanks are due to Franco Ruggieri for his valuable inputs.

10. References

10.1. Normative References

[RFC 2119] Bradner, S. "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[TF.460-5] ITU-R Recommendation TF.460-5 (1997): Standard-frequency and time-signal emissions.

[TF.536-1] ITU-R Recommendation TF.536-1 (1998): Time-scale notations.

[CWA 14167-2] CEN Workshop Agreement 14167-2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP).

[FIPS 140-1] FIPS PUB 140-1 (1994): Security Requirements for Cryptographic Modules.

[ISO 15408] ISO/IEC 15408 (1999) (parts 1 to 3): Information technology - Security techniques and Evaluation criteria for IT security.

10.2. Informative References

[CWA 14172] CEN Workshop Agreement 14172: EESSI Conformity Assessment Guidance.

[Dir 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[Dir 99/93/EC] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[ISO 17799] ISO/IEC 17799: Information technology Code of practice for information security management

[RFC 3126] Pinkas, D., Ross, J. and N. Pope, "Electronic Signature Formats for long term electronic signatures", RFC 3126, September 2001.

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

[TS 101733] ETSI Technical Specification TS 101 733 V.1.2.2 (2000-12) Electronic Signature Formats. Note: copies of ETSI TS 101 733 can be freely downloaded from the ETSI web site www.etsi.org.

[TS 101861] ETSI Technical Specification TS 101 861 V1.2.1. (2001-11). Time stamping profile. Note: copies of ETSI TS 101 861 can be freely downloaded from the ETSI web site www.etsi.org.

[TS 102023] ETSI Technical Specification TS 102 023. Policy requirements for Time-Stamping Authorities. Note: copies of ETSI TS 102 023 can be freely downloaded from the ETSI web site www.etsi.org.

[X.208] CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1), 1988.

Annex A (informative): Coordinated Universal Time

Coordinated Universal Time (UTC) is the international time standard that became effective on January 1, 1972. UTC has superseded Greenwich Mean Time (GMT), but in practice they are never more than 1 second different. Hence many people continue to refer to GMT when in fact they operate to UTC.

Zero (0) hours UTC is midnight in Greenwich, England, which lies on the zero longitudinal meridian. Universal time is based on a 24 hour clock, therefore, afternoon hours such as 4 pm UTC are expressed as 16:00 UTC (sixteen hours, zero minutes).

International Atomic Time (TAI) is calculated by the Bureau International des Poids et Mesures (BIPM) from the readings of more than 200 atomic clocks located in metrology institutes and observatories in more than 30 countries around the world. Information on TAI is made available every month in the BIPM Circular T (ftp://62.161.69.5/pub/tai/publication). It is that TAI does not lose or gain with respect to an imaginary perfect clock by more than about one tenth of a microsecond (0.0000001 second) per year.

Coordinated Universal Time (UTC): Time scale, based on the second, as defined and recommended by the International Telecommunications Radio Committee (ITU-R), and maintained by the Bureau International des Poids et Mesures (BIPM). The maintenance by BIPM includes cooperation among various national laboratories around the world. The full definition of UTC is contained in ITU-R Recommendation TF.460-4.

Atomic Time, with the unit of duration the Systeme International (SI) second defined as the duration of 9 192 631 770 cycles of radiation, corresponds to the transition between two hyperfine levels of the ground state of caesium 133. TAI is the International Atomic Time scale, a statistical timescale based on a large number of atomic clocks.

Universal Time (UT) is counted from 0 hours at midnight, with unit of duration the mean solar day, defined to be as uniform as possible despite variations in the rotation of the Earth.

- UT0 is the rotational time of a particular place of observation. It is observed as the diurnal motion of stars or extraterrestrial radio sources.

- UT1 is computed by correcting UT0 for the effect of polar motion on the longitude of the observing site. It varies from uniformity because of the irregularities in the Earth’s

rotation. UT1, is based on the somewhat irregular rotation of the Earth. Rotational irregularities usually result in a net decrease in the Earth's average rotational velocity, and ensuing lags of UT1 with respect to UTC.

Coordinated Universal Time (UTC) is the basis for international time-keeping and follows TAI exactly except for an integral number of seconds, 32 in year 2001. These leap seconds are inserted on the advice of the International Earth Rotation Service (IERS) (http://hpiers.obspm.fr/) to ensure that, having taken into account irregularities, the Sun is overhead within 0,9 seconds of 12:00:00 UTC on the meridian of Greenwich. UTC is thus the modern successor of Greenwich Mean Time, GMT, which was used when the unit of time was the mean solar day.

Adjustments to the atomic, i.e., UTC, time scale consist of an occasional addition or deletion of one full second, which is called a leap second. Twice yearly, during the last minute of the day of June 30 and December 31, Universal Time, adjustments may be made to ensure that the accumulated difference between UTC and UT1 will not exceed 0,9 s before the next scheduled adjustment. Historically, adjustments, when necessary, have usually consisted of adding an extra second to the UTC time scale in order to allow the rotation of the Earth to "catch up". Therefore, the last minute of the UTC time scale, on the day when an adjustment is made, will have 61 seconds. Adjustments dates are typically announced several months in advance in IERS Bulletin C: ftp://hpiers.obspm.fr/iers/bul/bulc/bulletinc.dat.

Coordinated Universal Time (UTC) differs thus from TAI by an integral number of seconds. UTC is kept within 0,9 s of UT1 by the introduction of one-second steps to UTC, the "leap second". To date these steps have always been positive.

Annex B (informative): Possible for Implementation Architectures and Time-Stamping Services

B.1. Managed Time-Stamping Service

Some organizations may be willing to host one or more Time-Stamping Units in order to take advantage of both the proximity and the quality of the Time-Stamping Service, without being responsible for the installation, operation and management of these Time-Stamping Units.

This can be achieved by using units that are installed in the premises from the hosting organization and then remotely managed by a Time-Stamping Authority that takes the overall responsibility of the quality of the service delivered to the hosting organization.

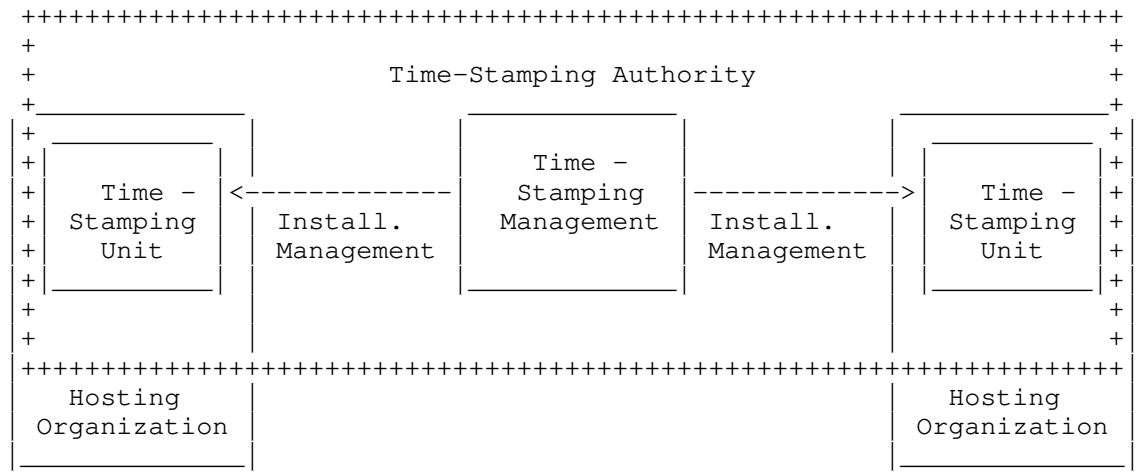

Figure B.1: Managed Time-stamping Service

The requirements for time-stamping services described in the current document includes requirements on both the time-stamping management and for the operation of the unit which issues the time-stamp tokens. The TSA, as identified in the time-stamp token, has the responsibility to ensure that these requirements are met (for example through contractual obligations).

It should be clear that the hosting organization will generally want to be able to monitor the use of the service and, at a minimum, know whether the service is working or not and even be able to measure the performances of the service, e.g., the number of time-stamps generated during some period of time. Such monitoring can be considered to be outside of TSA's time-stamping authority.

Therefore the description of the management operation described in the main body of the document is not limitative. Monitoring operations, if performed directly on the unit, may be permitted by the Time-Stamping service provider.

B.2. Selective Alternative Quality

Some relying parties may be willing to take advantage of particular characteristics from a time-stamp token such as a specific signature algorithm and/or key length or a specific accuracy for the time contained in the time stamp token. These parameters can be considered as specifying a "quality" for the time stamp token.

Time stamp tokens with various qualities may be issued by different time-stamping units operated by the same or different TSAs.

A particular time-stamping unit will only provide one combination of algorithm and key length (since a time-stamping unit is a set of hardware and software which is managed as a unit and has a single time-stamp token signing key). In order to obtain different combinations of algorithm and key length, different time-stamping units shall be used.

A particular time-stamping unit may provide a fixed accuracy for the time contained in the time stamp token or different accuracy if instructed to do so either by using a specific mode of access (e.g., e-mail or http) or by using specific parameters in the request.

Annex C (informative): Long Term Verification of Time-Stamp Tokens

Usually, a time-stamp token becomes unverifiable beyond the end of the validity period of the certificate from the TSU, because the CA that has issued the certificate does not warrant any more that it will publish revocation data, including data about revocations due to key compromises. However, verification of a time-stamp token might still be performed beyond the end of the validity period of the certificate from the TSU, if, at the time of verification, it can be known that:

- the TSU private key has not been compromised at any time up to the time that a relying part verifies a time-stamp token;
- the hash algorithms used in the time-stamp token exhibits no collisions at the time of verification;
- the signature algorithm and signature key size under which the time-stamp token has been signed is still beyond the reach of cryptographic attacks at the time of verification.

If these conditions cannot be met, then the validity may be maintained by applying an additional time-stamp to protect the integrity of the previous one.

The present document does not specify the details of how such protection may be obtained. For the time being, and until some enhancements are defined to support these features, the information may be obtained using-out-of bands means or alternatively in the context of closed environments. As an example, should a CA guaranty to maintain the revocation status of TSU certificates after the end of its validity period, this would fulfill the first requirement.

NOTE 1: An alternative to Time-Stamping is for a Trusted Service Provider to record a representation of a datum bound to a particular time in an audit trail, thus establishing evidence that the datum existed before that time. This technique, which is called Time-Marking, can be a valuable alternative for checking the long term validity of signatures.

NOTE 2: The TSA or other trusted third party service provider may support the verification of time-stamp tokens.

Annex D (informative): Model TSA Disclosure Statement Structure.

The TSA disclosure statement contains a section for each defined statement type. Each section of a TSA disclosure statement contains a descriptive statement, which MAY include hyperlinks to the relevant certificate policy/certification practice statement sections.

D.1. STATEMENT TYPE: Entire agreement

STATEMENT DESCRIPTION: A statement indicating that the disclosure statement is not the entire agreement, but only a part of it.

D.2. STATEMENT TYPE: TSA contact info

STATEMENT DESCRIPTION: The name, location and relevant contact information for the TSA.

D.3. STATEMENT TYPE: time-stamp token types and usage

STATEMENT DESCRIPTION: A description of each class/type of time-stamp tokens issued by the TSA (in accordance with each time-stamp policy) and any restrictions on time-stamp usage.

SPECIFIC REQUIREMENT: Indication of the policy being applied, including the contexts for which the time-stamp token can be used (e.g., only for use with electronic signatures), the hashing algorithms, the expected life time of the time-stamp token signature, any limitations on the use of the time-stamp token and information on how to verify the time-stamp token.

D.4. STATEMENT TYPE: Reliance limits.

STATEMENT DESCRIPTION: reliance limits, if any.

SPECIFIC REQUIREMENT: Indication of the accuracy of the time in the time-stamp token, and the period of time for which TSA event logs (see section 7.4.10) are maintained (and hence are available to provide supporting evidence).

D.5. STATEMENT TYPE: Obligations of subscribers.

STATEMENT DESCRIPTION: The description of, or reference to, the critical subscriber obligations.

SPECIFIC REQUIREMENT: No specific requirements identified in the current document. Where applicable the TSA may specify additional obligations.

D.6. STATEMENT TYPE: TSU public key status checking obligations of relying parties.

STATEMENT DESCRIPTION: The extent to which relying parties are obligated to check the TSU public key status, and references to further explanation.

SPECIFIC REQUIREMENT: Information on how to validate the TSU public key status, including requirements to check the revocation status of TSU public key, such that the relying party is considered to "reasonably rely" on the time-stamp token (see section 6.3).

D.7. STATEMENT TYPE: Limited warranty and disclaimer/Limitation of liability.

STATEMENT DESCRIPTION: Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs

SPECIFIC REQUIREMENT: Limitations of liability (see section 6.4).

D.8. STATEMENT TYPE: Applicable agreements and practice statement.

STATEMENT DESCRIPTION: Identification and references to applicable agreements, practice statement, time-stamp policy and other relevant documents.

D.9. STATEMENT TYPE: Privacy policy.

STATEMENT DESCRIPTION: A description of and reference to the applicable privacy policy.

SPECIFIC REQUIREMENT: Note: TSA's under this policy are required to comply with the requirements of Data Protection Legislation.

D.10. STATEMENT TYPE: Refund policy

STATEMENT DESCRIPTION: A description of and reference to the applicable refund policy.

D.11. STATEMENT TYPE: Applicable law, complaints and dispute resolution mechanisms.

STATEMENT DESCRIPTION: Statement of the choice of law, complaints procedure and dispute resolution mechanisms.

SPECIFIC REQUIREMENT: The procedures for complaints and dispute settlements. The applicable legal system.

D.12. STATEMENT TYPE: TSA and repository licenses, trust marks, and audit.

STATEMENT DESCRIPTION: Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm.

SPECIFIC REQUIREMENT: If the TSA has been assessed to be conformant with the identified time-stamp policy, and if so through which independent party.

Authors' Addresses

Denis Pinkas
Bull
Rue Jean Jaures,
78340 Les Clayes CEDEX
FRANCE

EMail: Denis.Pinkas@bull.net

Nick Pope
Security & Standards
192 Moulsham Street
Chelmsford, Essex
CM2 0LG
United Kingdom

EMail: pope@secstan.com

John Ross
Security & Standards
192 Moulsham Street
Chelmsford, Essex
CM2 0LG
United Kingdom

EMail: ross@secstan.com

This Informational RFC has been produced in ETSI ESI.

ETSI
F-06921 Sophia Antipolis, Cedex - FRANCE
650 Route des Lucioles - Sophia Antipolis
Valbonne - France
Tel: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
secretariat@etsi.fr
http://www.etsi.org

Contact Point

Claire d'Esclercs
ETSI
650 Route des Lucioles
F-06921 Sophia Antipolis, Cedex
FRANCE

EMail: claire.desclercs@etsi.org

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.