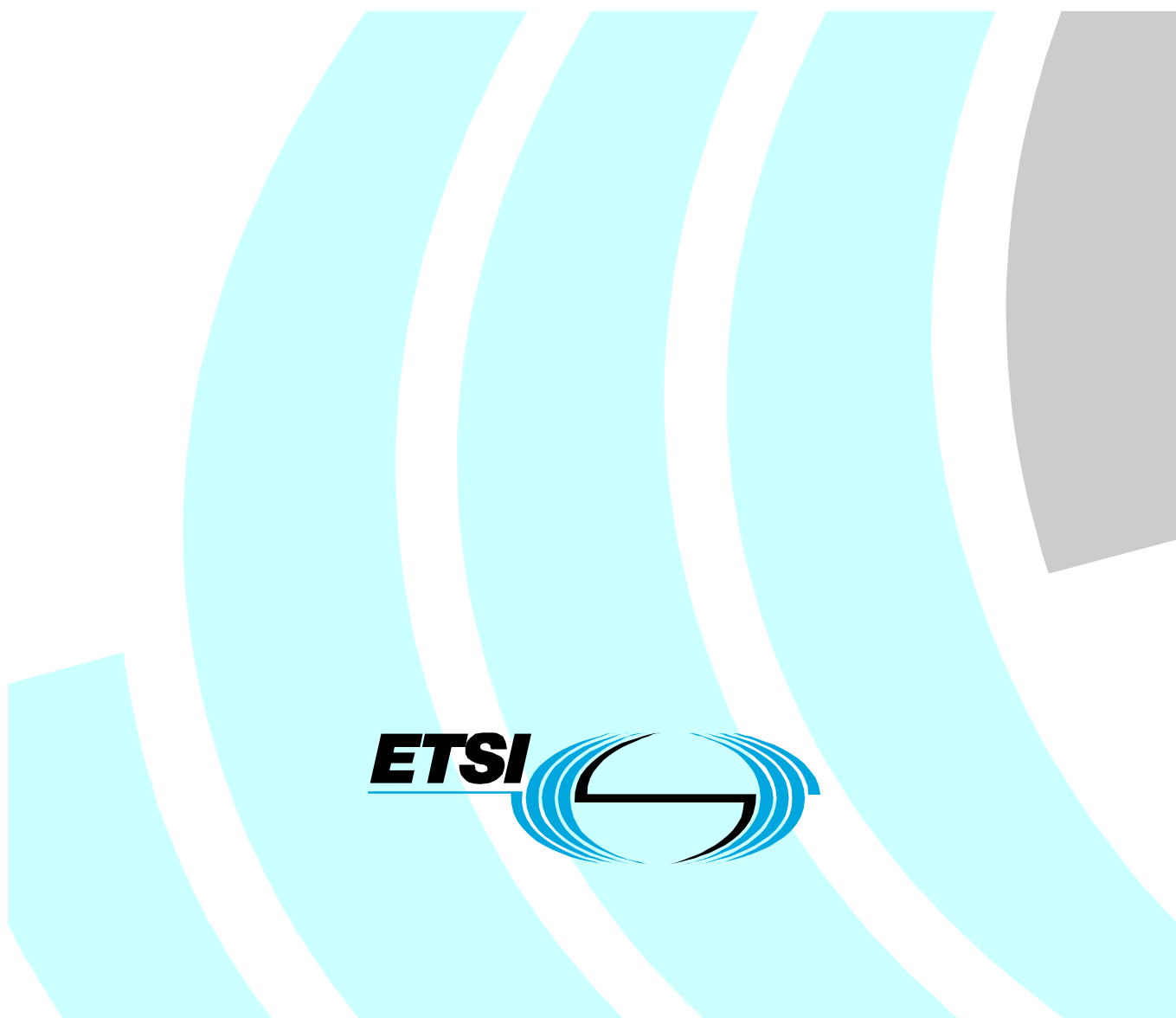


Policy requirements for time-stamping authorities



Reference

DTS/SEC-004005

Keywords

e-commerce, electronic signature, security, time-stamping, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, send your comment to:

editor@etsi.fr

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2002.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Introduction.....	5
1 Scope.....	6
2 References.....	6
3 Definitions and abbreviations.....	7
3.1 Definitions.....	7
3.2 Abbreviations.....	7
4 General concepts	8
4.1 Time-stamping services.....	8
4.2 Time-stamping authority.....	8
4.3 Subscriber.....	8
4.4 Time-stamp policy and TSA practice statement.....	8
4.4.1 Purpose.....	8
4.4.2 Level of specificity	9
4.4.3 Approach.....	9
5 Time-stamp Policies	9
5.1 Overview	9
5.2 Identification.....	9
5.3 User Community and applicability.....	10
5.4 Conformance.....	10
6 Obligations and liability.....	10
6.1 TSA obligations	10
6.1.1 General.....	10
6.1.2 TSA obligations towards subscribers.....	10
6.2 Subscriber obligations	10
6.3 Relying party obligations.....	11
6.4 Liability	11
7 Requirements on TSA practices	11
7.1 Practice and Disclosure Statements.....	11
7.1.1 TSA Practice statement	11
7.1.2 TSA disclosure Statement	12
7.2 Key management life cycle.....	13
7.2.1 TSA key generation	13
7.2.2 TSA private key protection.....	13
7.2.3 TSA public key Distribution.....	14
7.2.4 Rekeying TSA's Key.....	14
7.2.5 End of TSA key life cycle	14
7.2.6 Life cycle management of cryptographic module used to sign time-stamps	14
7.3 Time-stamping.....	15
7.3.1 Time-stamp token	15
7.3.2 Clock Synchronization with UTC.....	15
7.4 TSA management and operation	16
7.4.1 Security management.....	16
7.4.2 Asset classification and management.....	17
7.4.3 Personnel security.....	17
7.4.4 Physical and environmental security.....	18
7.4.5 Operations management.....	18
7.4.6 System Access Management	19
7.4.7 Trustworthy Systems Deployment and Maintenance.....	20
7.4.8 Compromise of TSA Services	20

7.4.9	TSA termination	21
7.4.10	Compliance with Legal Requirements	21
7.4.11	Recording of Information Concerning Operation of Time-stamping Services	22
7.5	Organizational.....	22
Annex A (informative):	Potential liability in the provision of time-stamping services	24
Annex B (informative):	Model TSA disclosure statement	25
B.1	Introduction.....	25
B.2	The TSA disclosure statement structure	26
Annex C (informative):	Coordinated Universal Time	27
Annex D (informative):	Long Term Verification of time-stamp token	28
Annex E (informative):	Possible for Implementation Architectures - Time-stamping Services	29
E.1	Managed Time-stamping Service.....	29
E.2	Selective Alternative Quality	29
Annex F (informative):	Bibliography.....	31
History	32

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Security (SEC).

Introduction

In creating reliable and manageable digital evidence it becomes necessary to have an agreed upon method of associating time data to transaction so that they might be compared to each other at some later time. The quality of this evidence is based in the process of 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.

In addition, in order to verify an electronic signature, it may be necessary to prove that the digital signature from the signer was applied when the signer's certificate was valid. This is necessary in two circumstances:

- 1) during the validity period of the signer's certificate, should the signer's private key be compromised and thus revoked for that reason;
- 2) after the end of the validity period of the signer's certificate, since CAs are not mandated to process revocation status information beyond the end of the validity period of the certificates they have issued.

Two generic methods exist to solve this problem. One consists to use a time-mark which is an audit record kept in a secure audit trail from a trusted third party which attaches a date to a signature value. This proves that the signature was generated before the date from the time-mark. This method is not the topic of the present document.

Another one consists to use a time-stamp which allows to prove that a datum existed before a particular time. This technique allows to prove that the signature was generated before the date contained in the time-stamp token. Policy requirements to cover that case is the primary reason of the present document.

However , it should be observed that these policy requirements allow to address other needs.

The electronic time stamp is gaining an increasing interest by the business sector and is becoming an important component of electronic signatures, also featured by the ETSI Electronic Signature Format standard TS 101 733, built upon the Time-Stamp protocol from the IETF (RFC 3161). Agreed minimum security and quality requirements are necessary in order to ensure trustworthy validation of long-term electronic signatures.

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

1 Scope

The present document specifies policy requirements relating to the operation of Time-stamping Authorities (TSAs). The present document defines policy requirements on the operation and management practices of TSAs such that subscribers and relying parties may have confidence in the operation of the time-stamping services.

These policy requirements are primarily 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 upon 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.

The current document addresses requirements for TSAs issuing time-stamp tokens which are synchronized with Coordinated universal time (UTC) and digitally signed by the TSA.

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).

The current document does not specify:

- protocols used to access the TSA;

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

- 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".

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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

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

[3] 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.

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

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

- [6] CWA 14167-2: "Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP)".

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 data to be time-stamped 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 [1].

NOTE: For most practical purposes UTC is equivalent to mean solar time at the prime meridian (0°). 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 C for more details).

UTC(k): Time-scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns. (See ITU-R Recommendation TF.536-1 [2]).

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
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 in the present document 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 provided is as specified by the TSA. This service component has responsibility 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 trusted by the users of the time-stamping services (i.e. subscribers as well as relying parties) to issue time-stamp tokens is called the Time-Stamping Authority (TSA). The TSA has overall responsibility for the provision of the time-stamping services identified in clause 4.1. The TSA's key is used to sign a time-stamp token and the TSA is identified in a time-stamp token as the issuer.

The TSA may make use of 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-stamps using the TSA's key. However, the private key or keys used to generate the time-stamp tokens are identified as belonging to the TSA which maintains overall responsibility for meeting the requirements defined in the current document.

A TSA may operate several identifiable time-stamping units. Each unit has a different key.

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 such an 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 clause 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

A time-stamp policy is a less specific document than a TSA practice statement. 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 the public key certificate of the TSA, 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 D on verification of the validity of a time-stamp token beyond the validity period of the TSA's certificate.

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

If an accuracy of better than 1 second is provided by the TSA then the accuracy shall be indicated in the TSA's disclosure statement (see clause 7.1.2) and in each time-stamp token issued to 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 clause 7.3.1).

5.2 Identification

The object-identifier 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)
```

A TSA shall also include the identifier for the time-stamp policy being supported in the TSA disclosure statement made available to subscribers and relying parties to indicate its claim of 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) but is generally applicable to any use which has a requirement for 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 clause 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 be conformant to the identified time-stamp policy by an independent party.

A conformant TSA must demonstrate that:

- a) it meets its obligations as defined in clause 6.1;
- b) it has implemented controls which meet the requirements specified in clause 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 clause 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 clause 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 TSA's certificate validity period, the validity of the signing key can be checked using current revocation status for the TSA's certificate. If the time of verification exceeds the end of the validity period of the corresponding certificate, see annex D 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.

For further details see annex A.

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 considered necessary to provide the necessary 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 minimising the restrictions on the techniques that a TSA may employ in issuing time-stamp tokens. In case of clause 7.4 (TSA management and operation) reference is made to other more general standards which may be used as 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 clause 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.
- 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 clause 6.2, if any.
- h) The relying party's obligations as defined in clause 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 clause 6.3) and any possible limitations on the validity period.
- j) The period of time during which TSA event logs (see clause 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 B. Alternatively this may be provided as part of a subscriber / relying party agreement. These TSA disclosure statement 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 TSA's signing key(s) shall be undertaken in a physically secured environment (see clause 7.4.4) by personnel in trusted roles (see clause 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 TSA's signing key(s) shall be carried out within a cryptographic module(s) which either:
 - meets the requirements identified in FIPS 140-1 [4] level 3 or higher, or
 - meets the requirements identified in CEN Workshop Agreement 14167-2 [6], or
 - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO 15408 [5], 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 TSA 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.

NOTE: See the document "Algorithms and parameters for Secure Electronic Signatures" (to be published by the Algorithms group (ALGO) working under the umbrella of EESSI-SG (European Electronic Signature Standardization Initiative Steering Group)) for general guidance on signature algorithms and key lengths.

7.2.2 TSA private key protection

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

In particular:

- a) The TSA private signing key shall be held and used within a cryptographic module which:
 - meets the requirements identified in FIPS 140-1 [4] level 3 or higher; or
 - meets the requirements identified in CEN Workshop Agreement 14167-2 [6]; or
 - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO 15408 [5], 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.

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

- b) If TSA 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 clause 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 TSA private signing keys shall be protected to ensure its confidentiality by the cryptographic module before being stored outside that device.

7.2.3 TSA public key Distribution

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

In particular:

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

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

- b) The TSA'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 TSA's Key

The life-time of TSA'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 clause 7.2.1c)).

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

- Clause 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 TSA's signing key. The longer the validity period of the TSA certificate will be, the longer the size of the records to be kept will be.
- Should a TSA private key be compromised, then the longer the life-time, the more affected time-stamp tokens there will be.

NOTE 2: TSA 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 TSA key life cycle

The TSA shall ensure that TSA 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 TSA's key expires.
- b) The TSA 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 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 TSA'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 clause 7.4.4);

- d) Time-stamp token signing cryptographic hardware is functioning correctly; and
- e) TSA private signing keys stored on TSA 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 TSA 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 clause 7.3.2c)) as being out of the stated accuracy (see clause 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.

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 TSA clock is not mandated.

- h) The name of the issuing TSA shall be identified in the time-stamp token. This 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 TSA clocks shall be maintained such that the clocks shall not be expected to drift outside the declared accuracy.
- b) The TSA 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 clause 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 C 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 administrative and management procedures are applied which 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 for guidance on information security management including information security infrastructure, management information security forum and information security policies. Other alternative guidance documents are given in annex F.

- 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 clause 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:

- a) 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 fulfil 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 clause 7.4.1).

NOTE 3: See ISO/IEC 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 TSA clock 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 offence 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 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 clause 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 co-ordinated 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 clause 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 clause 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 the TSA's private signing key 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 a TSA's private signing key or loss of calibration of the TSA 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 the TSA's operation (e.g. TSA key compromise), suspected compromise or loss of calibration the TSA 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 clause 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;
 - TSA 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 fulfil 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 its 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 [3], 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 TSA's signing key as appropriate for providing necessary legal evidence and as notified in the TSA disclosure statement (see clause 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.

TSA key management

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

Clock Synchronization

- k) Records concerning all events relating to synchronization of the TSA'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 clause 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.

Annex A (informative): Potential liability in the provision of time-stamping services

Liability derives from one of two sources: contract or statutory law (i.e. national law).

Where consumers are involved, statutory protections may also apply - specially the Unfair Contract Terms Directive (93/13/EEC) and the corresponding national implementations, which can even increment the level of protection.

These rules may constrain the TSA's capability to limit its liability, because the Directive prohibits terms that have not been individually negotiated which cause a significant imbalance in the parties' rights and obligations to the detriment of the consumer.

A national law can also establish additional restrictions on liability limitation.

Where these exceptions do not apply, a TSA may disclaim any or all warranties and limit its liability.

Annex B (informative): Model TSA disclosure statement

B.1 Introduction

The proposed model TSA disclosure statement is designed for use by a TSA issuing time-stamp tokens as a supplemental instrument of disclosure and notice. A TSA disclosure statement may assist a TSA to respond to regulatory requirements and concerns, particularly those related to consumer deployment. Further, the aim of the model TSA disclosure statement is to foster industry "self-regulation" and build consensus on those elements of a security policy and/or practice statement that require emphasis and disclosure.

Although security policy and practice statement documents are essential for describing and governing time-stamping policies and practices, many TSA users, especially consumers, may find these documents difficult to understand. Consequently, there is a need for a supplemental and simplified instrument that can assist TSA users in making informed trust decisions. Consequently, a TSA disclosure statement is not intended to replace a security policy or practice statement.

This annex provides an example of the structure for a TSA disclosure statement, illustrating the harmonized set of statement types (categories) that would be contained in a deployed time-stamping service.

B.2 The 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.

STATEMENT TYPES	STATEMENT DESCRIPTIONS	SPECIFIC REQUIREMENTS
Entire agreement	A statement indicating that the disclosure statement is not the entire agreement, but only a part of it.	
TSA contact info:	The name, location and relevant contact information for the TSA.	
time-stamp token types and usage:	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.	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.
Reliance limits:	The reliance limits, if any.	Indication of the accuracy of the time in the time-stamp token, and the period of time for which TSA event logs (see clause 7.4.10) are maintained (and hence are available to provide supporting evidence).
Obligations of subscribers:	The description of, or reference to, the critical subscriber obligations.	No specific requirements identified in the current document. Where applicable the TSA may specify additional obligations.
TSA public key status checking obligations of relying parties:	The extent to which relying parties are obligated to check the TSA public key status, and references to further explanation.	Information on how to validate the TSA public key status, including requirements to check the revocation status of TSA public key, such that the relying party is considered to "reasonably rely" on the time-stamp token (see clause 6.3).
Limited warranty and disclaimer/Limitation of liability:	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	Limitations of liability (see clause 6.4).
Applicable agreements and practice statement	Identification and references to applicable agreements, practice statement, time-stamp policy and other relevant documents.	
Privacy policy:	A description of and reference to the applicable privacy policy.	Note: TSA's under this policy are required to comply with the requirements of Data Protection Legislation.
Refund policy:	A description of and reference to the applicable refund policy.	
Applicable law, complaints and dispute resolution:	Statement of the choice of law, complaints procedure and dispute resolution mechanisms.	The procedures for complaints and dispute settlements; The applicable legal system.
TSA and repository licenses, trust marks, and audit:	Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm.	If the TSA has been assessed to be conformant with the identified time-stamp policy, and if so through which independent party.

Annex C (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.

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 D (informative): Long Term Verification of time-stamp token

Usually, a time-stamp token becomes unverifiable beyond the end of the validity period of the certificate from the TSA, 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 TSA, if, at the time of verification, it can be known that:

- the TSA 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. Alternatively the time-stamped data may be placed in secure storage.

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 TSA certificate after the end of its validity period, this would fulfil 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 E (informative): Possible for Implementation Architectures - Time-stamping Services

E.1 Managed Time-stamping Service

Some organizations may be willing to host one or more Time-Stamping Authorities and 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 Authorities.

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 Service provider that takes the overall responsibility of the quality of the service delivered to the hosting organization.

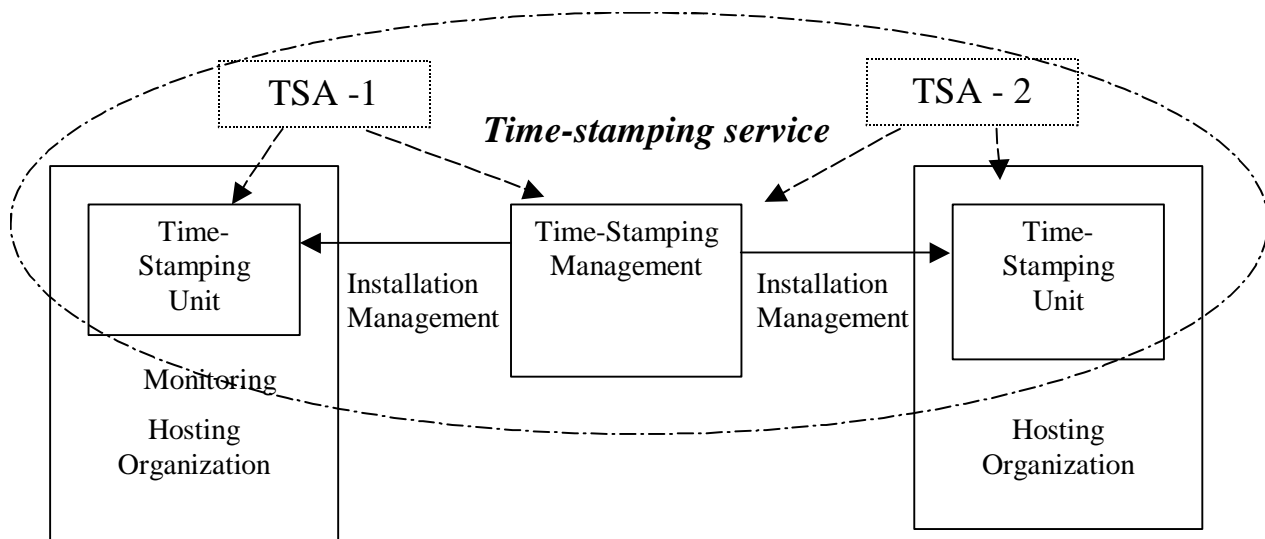


Figure E.1: Managed Time-stamping Service

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 service.

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.

E.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 F (informative): Bibliography

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts - Statement by the Council and the Parliament re Article 6 (1) - Statement by the Commission re Article 3 (1), first indent.

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

RFC 3161(2001) Internet X.509: "Public Key Infrastructure: Time-Stamp Protocol (TSP)".

Algorithms and parameters for Secure Electronic Signatures" (to be published by the Algorithms group (ALGO) working under the umbrella of EESSI-SG (European Electronic Signature Standardization Initiative Steering Group).

ISO/IEC 14516: "Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services".

ISO/IEC TR 13335-1 (1996): "Information technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security".

ISO/IEC TR 13335-2 (1997): "Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security".

ISO/IEC TR 13335-3 (1998): "Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security".

ISO/IEC TR 13335-4 (2000): "Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards".

ITU-R Recommendation TF.460-4: "Standard-frequency and time-signal emissions".

ETSI TS 101 733: "Electronic signature formats".

ETSI TS 101 861: "Time stamping profile".

ISO/IEC 17799: "Information technology - Code of practice for information security management".

History

Document history		
V1.1.1	January 2002	Publication