TC TrustCenter GmbH
Time-Stamp Policy

Version 1.1 of January 21, 2008

TC TrustCenter
Time-stamp Policy

Version 1.1 of January 21, 2008

Introduction

TC TrustCenter is a Certification Services Provider offering certificates (advanced certificates as well as qualified certificates) and qualified as well as non-qualified (advanced) time-stamps. Qualified certificates and qualified time-stamps are compliant with the German Signature Act and the Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [EU-DIR] and have the same effect in legal transactions as a handwritten signature.

A time-stamp proves the existence of digital data at a specific time in a trustworthy and traceable manner. Time-stamped data can not be altered unnoticed.

Data to be time-stamped can be sent to the time-stamping service. Out of this data the time-stamping service generates an object consisting of the hash value of the data and the actual time. The time-stamping service then electronically signs this object thereby protecting its integrity.

This document contains TC TrustCenter's Time-stamp Policy, describing general rules which shall be followed by the time-stamping service, and TC TrustCenter's Time-stamp Practice Statement, describing how processes and procedures implement these rules.

Time-stamps supported by this document and issued by TC TrustCenter may be used to document that any data bearing such a time-stamp already existed at the time specified by the time-stamp (e.g. a contract has been closed before a given time).

This document specifies the practices of the operation and management of TC TrustCenter's CAs issuing time-stamps in accordance with the Directive 1999/93/EC, in accordance with the German Signature Act, and in accordance with the European Telecommunications Standards Institute's Technical Specification 102 023 (ETSI TS 101 456): Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

Structure and content of this document comply with ETSI standard ETSI TS 102 023 [ETSI].

It is common practice for a CA (Certification Authority) or TSA (Time-stamping Authority) to have two documents in place:

- a Policy stating the requirements on a specific service thus allowing an estimation of the trustworthiness and reliability of certificate contents or time-stamps,
- a Practice Statement describing the practices which a CA or TSA employs to implement the requirements laid down in the Policy.

This document considers qualified time-stamps as well as other time-stamps. Though qualified time-stamps underlie the regulations and requirements defined in the Directive 1999/93/EC [EU-DIR] and in the German Signature Act [GSA], and other "non-qualified" or "advanced" time-stamps do not underlie these requirements, TC TrustCenter uses the same infrastructure to issue both kinds of time-stamps. (Time-stamps issued under the policy of Adobe's Certified Document Services are advanced time-stamps; this is not a third type of time-stamps).

Since the infrastructure is identical, TC TrustCenter decided not to publish two different policies (one for each type of time-stamp). There is only one policy for all time-stamps.

Furthermore, both above mentioned documents (Policy and Practice Statement) have been merged into one single document, this Time-stamp Policy (TP) and Time-stamp Practice Statement (TPS).

This TP/TPS in combination with TC TrustCenter's organization, processes, and procedures will be assessed by independent auditors to be compliant to the standard „ETSI TS 101 023 – Policy requirements for time-stamping authorities" of the European Telecommunications Standards Institute (ETSI).

1 Scope

The present document specifies policy requirements relating to the operation of a Time-Stamping Authority (TSA) and defines the operation and management practices of TC TrustCenter's TSA such that subscribers and relying parties may have confidence in the operation of the time-stamping services.

The structure and contents of this Time-stamp Policy are laid out in accordance with ETSI TS 102 023 V1.2.1 (2003-01), Policy Requirements for time-stamping authorities. This Time-stamp Policy is administered and approved by TC TrustCenter's Policy and Practices Board (PPB). It should be read in conjunction with TC TrustCenter's Certification Practice Statements (CPS) which can be downloaded from http://www.trustcenter.de/repository.

The 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 and with the German Signature Act [EU-DIR]) but may be applied to any application requiring to prove that the data under consideration existed before a particular time.

The policy requirements are based upon the use of public key cryptography, public key certificates and reliable time sources.

Subscriber and relying parties should consult the TC TrustCenter Time-Stamp Practice and Disclosure Statement of this document to obtain further details of precisely how this time-stamp policy is implemented by TC TrustCenter.

The current document does not specify:

- protocols used to access the time-stamping service;
- how the requirements on protocols may be assessed by an independent body;
- requirements for information to be made available to such independent bodies;
- requirements on such independent bodies.

2 References

[CEN] CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".

[ETSI] ETSI TS 102 023, V1.2.1 (2003-01), Policy Requirements for time-stamping authorities

[ETSI-TS] ETSI TS 101.861, V1.2.1 (2002-03), Time Stamping Profile

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

EU-PROT 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.

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

[GSA] Law Governing Framework Conditions for Electronic Signatures of 16 May 2001 (Federal Law Gazette I, p. 876), last amended by Art. 1 of the First Act Amending the Signature Law (First Signature Amendment Act - 1. SigÄndG) of 4 January 2005 (Federal Law Gazette I, p. 2) (http://www.bundesnetzagentur.de/media/archive/3612.pdf)

[GDSO] Ordinance on electronic Signatures (Signaturverordnung, SigV) http://www.bundesnetzagentur.de/media/archive/3613.pdf

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

[TC-CPS] TC TrustCenter GmbH, Certification Practice Statement Version 1.6, July 5, 2007 http://www.trustcenter.de/cps

3 Definitions and Abbreviations

3.1 Definitions

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

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

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-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 (TSA): 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-stamp services

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.

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).

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).

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

CPS	Certification Practice Statement
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
NTP	Network Time Protocol
OID	Object Identifier
PTB	Physikalisch-Technische Bundesanstalt (http://www.ptb.de)
RFC	Request for Comments
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest Shamir Adleman Algorithm
SHA	Secure Hash Algorithm
TSA	Time-stamping Authority
TSU	Time-stamping Unit
UTC	Coordinated Universal Time

4 General Concepts

4.1 Time-stamp services

The provision of time-stamp 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-stamp 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-stamp services.

4.2 Time-Stamping Authority

The authority trusted by the users of the time-stamp services (i.e. subscribers as well as relying parties) to issue time-stamp tokens is called the Time-stamping Authority (TSA). The TSA shall have the overall responsibility for the provision of the time-stamp services identified in section 4.1. The TSA shall have responsibility for the operation of one or more TSU's which create and sign on behalf of the TSA. The TSA responsible for issuing a time-stamp token shall be identifiable (see section 7.3.1).

The TSA may make use of other parties to provide parts of the time-stamp services. However, the TSA shall always maintain overall responsibility and ensure 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 shall identified as belonging to the TSA which shall maintain overall responsibility for meeting the requirements defined in the current document.

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

A TSA is a certification-service-provider, as defined in the EU Directive on Electronic Signatures (see [EU-DIR] 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 shall be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization is expected to suitably inform its end users.

When the subscriber is an end-user, the end-user shall 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.

4.4.1 Purpose

In general, a time-stamp policy states "what is to be adhered to", while the 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 clocks. 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 is a combination of both; the time-stamp policy and the time-stamp practice statement.

TC TrustCenter's Time-stamp Policy specifies which general requirements for trusted time-stamp services shall be met (sections 5 to 7).

TC TrustCenter's TSA Practice Statement states 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. TC TrustCenter's TSA Practice Statement is a more detailed description of the terms and conditions as well as business and operational practices of TC TrustCenter's TSA in issuing and otherwise managing time-stamp services. TC TrustCenter's TSA Practice Statement enforces the rules established by TC TrustCenter's Time-Stamp Policy. The Time-stamp Practice Statement defines how TC TrustCenter's TSA meets the technical, organizational, and procedural requirements identified TC TrustCenter's Time-Stamp Policy.

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 time-stamp services, whereas the TSA practice statement is always defined by the provider.

5 Time-Stamp Policy

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 applications with common security requirements" (see sections 3.1 and 4.4).

This section of the document defines the requirements which shall be fulfilled by TC TrustCenter's TSA when issuing time-stamp tokens.

TC TrustCenter's TSA shall issue time-stamps in compliance with the specifications in ETSI TS 102 023 [ETSI] and in compliance with TC TrustCenter's Time-stamp Policy (this document).

The content of ETSI TS 102 023 is technically equivalent to RFC 3628: Requirements for Time-Stamping Authorities.

5.2 Identification

TC TrustCenter issues several types of time-stamps. Currently these are:

- Qualified time-stamps
- Advanced time-stamps

- Time-stamps for Adobe Certified Document Services.

The requirements for all these time-stamps have been merged into one document (this time-stamp policy).

To distinguish between different time-stamps each type of time-stamp has been assigned its own OID:

The object-identifier for support of qualified time-stamps is:

> iso(1) member-body(2) de(276) din-certco(0) trustcenter(44) Basis policies(1) time-stamp-policies(2) SigG(1).

The object-identifier for support of advanced time-stamps is:

> iso(1) member-body(2) de(276) din-certco(0) trustcenter(44) Basis policies(1) time-stamp-policies(2) Advanced(3).

The object-identifier for support of Adobe Certified Document Services is:

> OID=1.2.840.113583.1.2.1.

TC TrustCenter shall include the appropriate OID in each time-stamp object issued.

5.3 User Community and applicability

This policy is aimed at meeting

- the requirements of time-stamping qualified electronic signatures (see [EU-DIR]) for long term validity (OID 1.2.276.0.44.1.2.1),
- the requirements of time-stamping for Adobe Certified Document Services (OID 1.2.840.113583.1.2.1), and
- the requirements of ETSI TS 102 023 (OID 1.2.276.0.44.1.2.3) for 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

TC TrustCenter shall use the identifiers in section 5.2 for the time-stamp policy in time-stamp tokens.

TC TrustCenter shall further constraint the requirements identified in this policy

> a) if TC TrustCenter claims conformance to other more restrictive time-stamp policies and makes available to subscribers and relying parties on request the evidence to support the claim of conformance; or
>
> b) if TC TrustCenter has been assessed to be conformant to other more restrictive time-stamp policies by an independent party.

In order to prove conformance TC TrustCenter shall:

a) meet its obligations as defined in section 6.1;

b) implement controls which meet the requirements specified in section 7.

TC TrustCenter is subject to periodic independent external audits to demonstrate conformance with

- the German Signature Act,
- TC TrustCenter acting as a CSP for Identrust Level One Participants,
- MBA/SISAC (Secure Identity Services Accreditation Corporation, a subsidiary of the Mortgage Bankers Association of America),
- ETSI TS 101 456,
- ETSI TS 102 042, and
- ETSI TS 102 023.

ETSI TS 102 042 is in many cases accepted as an equivalent to the WebTrust™ program for Certification Authorities. ETSI TS 101 456 is a standard for compliance with European regulations for issuing qualified certificates and qualified time-stamps.

6 Obligations and liability

6.1 TSA obligations

6.1.1 General

TC TrustCenter shall ensure that all requirements, as detailed in section 7, are implemented as applicable to the time-stamp policy in this document.

TC TrustCenter shall ensure conformance with the procedures prescribed in this policy, even when the TSA functionality (or parts of it) is undertaken by sub-contractors.

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

TC TrustCenter shall provide all its time-stamping services consistent with the Time-stamp Practice Statement in this document.

6.1.2 TSA obligations towards subscribers

The TSA shall meet its claims as given in this document.

TC TrustCenter shall provide permanent access to the time-stamping service except during maintenance intervals and except during periods where a reliable time source is not available or other events that do not lie in TC TrustCenter's sphere of influence (force majeure, war, strike, governmental restrictions, etc.).
Planned maintenance windows shall be contractually agreed upon with the subscriber or they shall be announced on TC TrustCenter's website.

Furthermore, TC TrustCenter shall

- implement and operate a reliable and trustworthy infrastructure for information exchange and communication,
- respect the role of trademarks and intellectual property,
- offer its time-stamping services in compliance with commonly accepted standards as described in section 5.1 „Overview“,
- issue only correct time-stamps, and

- use a time source with a deviation from German Legal Time of less than one second.

6.2 Subscriber obligations

When obtaining a time-stamp token the subscriber shall verify 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.

This policy places no further obligations on the subscriber.

Additional requirements can be laid down in contractual agreements between TC TrustCenter and subscribers.

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, the relying party 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;

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.

After expiry of the time-stamp certificate, the relying party should:

– verify that the TSU private key is not revoked, and
– verify that the cryptographic hash function and the signing algorithm used in the time-stamp token are still considered secure.

6.4 Liability

TC TrustCenter shall operate its TSA in accordance with this Time-Stamp Policy, its CPS, and the terms of service level agreements with subscribers. TC TrustCenter shall make no further representations or warranties relating to the availability or accuracy of the time-stamping service.

TC TrustCenter shall not be liable for matters that lie outside its sphere of influence and responsibility.

TC TrustCenter shall be only liable as stipulated by the applicable law. As a certification services provider issuing qualified certificates and qualified time-stamps to the public TC TrustCenter's liability for qualified time-stamps is specified in § 11 of the German Signature Act.

As a certification services provider under the German Signature Act TC TrustCenter is obliged to make appropriate cover provisions to ensure to be able to meet the statutory obligations for reimbursement of damages caused by an infringement.

7 Requirements on TSA Practices

TC TrustCenter's TSA shall implement the controls that meet the following requirements.

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.

7.1 Practice and Disclosure Statements

7.1.1 TSA Practice statement

TC TrustCenter's 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.

c) TC TrustCenter's Time-stamp 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.

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 data 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 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.

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

7.2 Key management life cycle

7.2.1 TSA key generation

TC TrustCenter's 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 assigned to the specific roles under TC TrustCenter's role concept.

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 PUB 140-1 [FIPS] level 3 or higher, or

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

   - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [ISO], 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 TC TrustCenter's TSA.

7.2.2 TSU private key protection

TC TrustCenter's 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 PUB 140-1 [FIPS] level 3 or higher; or
   - meets the requirements identified in CEN Workshop Agreement 14167-2 [CEN]; or
   - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [ISO], 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.

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 assigned to the specific roles under TC TrustCenter's role concept.

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

TC TrustCenter's 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.

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-stamp policy.

7.2.4 Rekeying TSU's Key

The life-time of TC TrustCenter's 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 7.2.1 c.).

7.2.5 End of TSU key life cycle

TC TrustCenter's 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 Time-stamp token generation system shall reject any attempt to issue Time-stamp tokens 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 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

TC TrustCenter's 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 an UTC(k) laboratory.

d. The time included in the time-stamp token shall be synchronized with UTC within the accuracy defined in this policy (see section 6.1.2) and, if present, within the accuracy defined in the time-stamp token itself.

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

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

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

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

TC TrustCenter 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.

c. TC TrustCenter 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 7.3.1 e.).

d. TC TrustCenter 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.

7.4 TSA management and operation

7.4.1 Security management

TC TrustCenter shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized best practice.

In particular:

a) TC TrustCenter 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 TC TrustCenter and appropriate arrangements made to ensure that third parties are bound to implement any controls required by TC TrustCenter's TSA. TC TrustCenter shall retain responsibility for the disclosure of relevant practices of all parties.

b) TC TrustCenter's management shall provide direction on information security through a suitable high level steering forum that is responsible for defining the TC TrustCenter 's information security policy. TC TrustCenter 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 TC TrustCenter shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by TC TrustCenter's management forum.

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

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

7.4.2 Asset classification and management

TC TrustCenter shall ensure that its information and other assets receive an appropriate level of protection.

In particular: TC TrustCenter's 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

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

In particular:

a. TC TrustCenter shall employ personnel who possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.

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

c. TC TrustCenter's 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 TC TrustCenter's TSA information security management procedures (see section 7.4.1).

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. TC TrustCenter's TSA personnel shall be formally appointed to trusted roles by senior management responsible for security.

i. TC TrustCenter's 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.

7.4.4 Physical and environmental security

TC TrustCenter 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 sections 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. TC TrustCenter'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.

7.4.5 Operations management

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

In particular:

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.

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 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. TC TrustCenter's TSA security operations shall be separated from other operations.

The 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.

Except housekeeping these operations shall be managed by TC TrustCenter's trusted personnel. Housekeeping may actually be performed by, non-specialist, operational personnel (under supervision).

7.4.6 System Access Management

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

In particular:

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.

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 TC TrustCenter'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. TC TrustCenter's TSA personnel shall be accountable for their activities, for example by retaining event logs (see section7.4.10).

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 TC TrustCenter.

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

7.4.7 Trustworthy Systems Deployment and Maintenance

TC TrustCenter's TSA shall use trustworthy systems and products that are protected against modification.

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 TC TrustCenter's 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

TC TrustCenter's 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.

7.4.9 TSA termination

TC TrustCenter's 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 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 the TSU's certificates revoked.

7.4.10 Compliance with Legal Requirements

TC TrustCenter's TSA shall ensure compliance with legal requirements.

In particular:

a. The TSA shall ensure that the requirements of the European data protection Directive [EU-DIR], 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 service

TC TrustCenter's 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.
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.
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

TC TrustCenter's 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.

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.

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.