SLOVENSKI STANDARD
SIST-TS ETSI/TS 102 023 V1.2.1:2005

01-maj-2005

Elektronski podpisi in infrastruktura (ESI) ï Politika zahtev za organe za ļ asovno ģigosanje

Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities

Ta slovenski standard je istoveten z: **TS 102 023 Version 1.2.1**

ICS:

35.040	Nabori znakov in kodiranje informacij	Character sets and information coding

SIST-TS ETSI/TS 102 023 V1.2.1:2005 **en**

ETSI TS 102 023 V1.2.1 (2003-01)

Technical Specification

Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities

Reference
RTS/ESI-000014

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.org

Copyright Notification

Contents

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).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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 TSUs.

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

The current document does not specify:

- protocols used to access the TSUs;

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 14172-2 [6].

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.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[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] 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)".

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

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

3 Definitions and abbreviations

3.1 Definitions

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

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

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

subscriber: entity requiring the services provided 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-stamping 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). (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).

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:

BIPM	Bureau International des Poids et Mesures
GMT	Greenwich Mean Time
IERS	International Earth Rotation Service
TAI	International Atomic Time
TSA	Time-Stamping Authority
TST	Time-Stamp token
TSU	Time-Stamping Unit
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 has responsibility for the operation of one or more TSU's which creates and signs on behalf of the TSA. The TSA responsible for issuing a time-stamp token is identifiable (see clause 7.3.1 h)).

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-stamp tokens using the TSU's keys. 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 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 public key certificates, with an accuracy of 1 second or better.

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

A TSA may define its own policy which enhances the policy defined in 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(02023)  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.