Draft ETSI EN 319 421 V1.0.0 (2015-06)

Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

Reference

DEN/ESI-0019421

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Introduction 5
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 8
3 Definitions and abbreviations 9
3.1 Definitions 9
3.2 Abbreviations 9
4 General concepts 10
4.1 General policy requirements concepts 10
4.2 Time-stamping services 10
4.3 Time-Stamping Authority (TSA) 10
4.4 Subscriber 10
4.5 Time-stamp policy and TSA practice statement 11
5 Introduction to time-stamp policies and general requirements 11
5.1 General 11
5.2 Identification 11
5.3 User community and applicability 11
5.3.1 Best practices time-stamp policy 11
6 Policies and practices 12
6.1 Risk assessment 12
6.2 Trust Service Practice Statement 12
6.3 Terms and conditions 12
6.4 Information security policy 12
6.5 TSA obligations 12
6.5.1 General 12
6.5.2 TSA obligations towards subscribers 12
6.6 Information for relying parties 13
7 TSA management and operation 13
7.1 Introduction 13
7.2 Internal organization 13
7.3 Personnel security 13
7.4 Asset management 13
7.5 Access control 14
7.6 Cryptographic controls 14
7.6.1 General 14
7.6.2 TSU key generation 14
7.6.3 TSU private key protection 14
7.6.4 TSU public key certificate 15
7.6.5 Rekeying TSU's key 15
7.6.6 Life cycle management of signing cryptographic hardware 15
7.6.7 End of TSU key life cycle 15
7.7 Time-stamping 16
7.7.1 Time-stamp issuance 16
7.7.2 Clock synchronization with UTC 16
7.8 Physical and environmental security 17
7.9 Operation security 17
7.10 Network security 18
7.11 Incident management 18

7.12 Collection of evidence 18
7.13 Business continuity management 18
7.14 TSA termination and termination plans 18
7.15 Compliance 19

8 Additional requirements for Regulation (EU) No 910/2014 19
8.1 TSU public key certificate 19

Annex A (informative): Potential liability in the provision of time-stamping services 20

Annex B (informative): Model TSA disclosure statement 21

B.1 Introduction 21

B.2 TSA disclosure statement structure 22

Annex C (informative): Coordinated Universal Time (UTC) 23

Annex D (informative): Long term verification of time-stamps 24

Annex E (informative): Regulation (EU) No 910/2014 and qualified electronic time-stamp policy cross-reference 25

Annex F (informative): Possible implementation architectures - time-stamping service 26

F.1 Managed time-stamping service 26

F.2 Selective alternative quality 26

Annex G (informative): Major changes from ETSI TS 102 023 28

Annex H (informative): Conformity Assessment Check list 29

History 30

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://ipr.etsi.org).

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 draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document was previously published as ETSI TS 102 023 [i.8].

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	12 months after doa

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.4].

The Regulation includes requirements for Trust Service Providers (TSP) providing services to the public, including TSPs issuing time-stamps. Additionally, more specific requirements are identified in the Regulation for a specific class of TSP called a Qualified TSP, with further specific requirements for those Qualified TSPs which issue qualified time-stamps. The present document is aimed to meet the requirements of the Regulation for both Qualified and non-Qualified TSPs issuing Qualified and non-Qualified electronic time-stamps respectively.

In order to verify an electronic signature, it can be necessary to prove that the 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 certificate be revoked before the end of its validity, e.g. because the signer's private key has been compromised;

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.

One method consists to use a time-stamp which allows proving that a datum existed before a particular time. This technique allows proving that the signature was generated before the date contained in the time-stamp. Policy requirements to cover that case are the primary aim of the present document.

However, these policy requirements allow addressing other needs.

Time-stamping is gaining an increasing interest by the business sector and is becoming an important component of digital signatures, this is commonly based upon the Time-Stamp protocol from the IETF RFC 3161 [i.2] which is profiled in ETSI EN 319 422 [5]. Agreed minimum security and quality requirements are necessary in order to ensure trustworthy validation of long-term digital signatures.

1 Scope

The present document specifies policy and security requirements relating to the operation and management practices of TSPs issuing time-stamps.

These policy requirements are applicable to TSPs issuing time-stamps. Such time-stamps can be used in support of digital signatures or for any application requiring to prove that a datum existed before a particular time.

The present document can be used by independent bodies as the basis for confirming that a TSP can be trusted for issuing time-stamps.

The present document does not specify:

- protocols used to access the TSUs;

NOTE 1: A time-stamping protocol is defined in IETF RFC 3161 [i.2] including optional update in IETF RFC 5816 [i.3] and profiled in ETSI EN 319 422 [5].

- how the requirements identified herein can 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 ETSI EN 319 403 [i.10].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.Not applicable.

[1] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".

[2] ISO/IEC 19790:2006: "Information technology -- Security techniques -- Security requirements for cryptographic modules".

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

[4] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[5] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp profiles".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EN 319 122: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.2] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

[i.3] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

[i.4] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

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

[i.6] BIPM Circular T.

NOTE: Available from the BIPM website http://www.bipm.org/.

[i.7] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.8] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

[i.9] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

[i.10] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.11] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.12] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.13] CEN EN 419 231: "Protection profile for trustworthy systems supporting time stamping".

[i.14] CEN EN 419 221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup ".

[i.15] CEN EN 419 221-3: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for Cryptographic module for CSP key generation services ".

[i.16] CEN EN 419 221-4: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup".

[i.17] CEN EN 419 221-5: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given ETSI EN 319 401 [4] and the following 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.

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 [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).

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

subscriber: legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations

time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

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

NOTE: This is a specific type of trust service policy as defined in ETSI EN 319 401 [4].

trust service: electronic service that enhances trust and confidence in electronic transactions

Trust Service Provider (TSP): entity which provides one or more trust services

Time-Stamping Authority (TSA): TSP which issues time-stamps using one or more time-stamping units

Time-Stamping Unit (TSU): set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time

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

NOTE: This is a specific type of trust service practice statement as defined in ETSI EN 319 401 [4].

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

UTC(k): time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.

NOTE: A list of UTC(k) laboratories is given in clause 1 of Circular T [i.6] disseminated by BIPM and available from the BIPM website (http://www.bipm.org/).

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 401 [4] and the following apply:

BIPM	Bureau International des Poids et Mesures
BTSP	Best practices Time-Stamp Policy
CA	Certification Authority
GMT	Greenwich Mean Time
IERS	International Earth Rotation and Reference System Service
IT	Information Technology

TAI	International Atomic Time
TSA	Time-Stamping Authority
TSP	Trust Service Providers
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

4 General concepts

4.1 General policy requirements concepts

The present document references ETSI EN 319 401 [4] for generic policy requirements common to all classes of trust service providers service.

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

Subscriber and relying parties are expected to 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).

4.2 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-stamps.
- **Time-stamping management:** This service component 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.

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 present document and places no restrictions on any subdivision of an implementation of time-stamping services.

4.3 Time-Stamping Authority (TSA)

A Trust Service Provider (TSP) providing time-stamping services to the public, is called the Time-Stamping Authority (TSA). The TSA has overall responsibility for the provision of the time-stamping services identified in clause 4.2. The TSA has responsibility for the operation of one or more TSUs which creates and signs on behalf of the TSA. The TSA responsible for issuing a time-stamp is identifiable (see clause 7.7.1, d).

The TSA may make use of other parties to provide parts of the time-stamping services. However, the TSA always maintains overall responsibility (as per clause 6.5) and ensures that the policy requirements identified in the present document are met.

EXAMPLE: A TSA sub-contracts all the component services, including the services which generate time-stamps using the TSU's keys. However, the private key or keys used to generate the time-stamps are identified as belonging to the TSA which maintains overall responsibility for meeting the requirements defined in the present document.

A TSA may operate several identifiable time-stamping units.

A TSA is a trust service provider as described in ETSI EN 319 401 [4] which issues time-stamps.

4.4 Subscriber

When the subscriber is an organization, it comprises several end-users or an individual end-user and 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.

4.5 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.

A time-stamp policy is a form of Trust Service Policy as specified in ETSI EN 319 401 [4] applicable to trust service providers issuing time-stamps.

TSA Practice Statement is a form of Trust Service Practice Statement as specified in ETSI EN 319 401 [4] applicable to trust service providers issuing time-stamps.

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.

5 Introduction to time-stamp policies and general requirements

5.1 General

The policy requirements are defined in the present document in terms of a time-stamp policy. The present document specifies one time-stamp policy: a best practices time-stamp policy (BTSP) for TSAs issuing time-stamps, supported by public key certificates, with an accuracy of 1 second or better.

A TSA may define its own policy which enhances a policy defined in the present document. Such a policy shall incorporate or further constrain the requirements identified in the present 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 6.3) and in each time-stamp issued to an accuracy of better than 1 second.

5.2 Identification

The identifier of the time-stamp policy specified in the present document is:

a) BTSP : a best practices policy for time-stamp.

```
itu-t(0) identified-organization(4) etsi(0)
time-stamp-policy(2023)
policy-identifiers(1) baseline-ts-policy (1)
```

By including this object identifier in a time-stamp, the TSA claims conformance to the identified time-stamp policy.

A TSA shall 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.

When the TSA uses its own identifier for the time-stamp policy, the TSA shall indicate in its policy document and in its TSA disclosure statement, the ETSI time-stamping identifier (i.e. BSTP) being supported.

5.3 User community and applicability

5.3.1 Best practices time-stamp policy

This policy is aimed at meeting the requirements of time-stamp for long term validity (e.g. as defined in ETSI EN 319 122 [i.1]) 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.