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

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://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.

6 Policies and practices

6.1 Risk assessment

The requirements identified in ETSI EN 319 401 [4], clause 5 shall apply.

6.2 Trust Service Practice Statement

The requirements identified in ETSI EN 319 401 [4], clause 6.1 shall apply.

In addition, the statement shall at least specify for each time-stamp policy supported by the TSA:

a) at least one hashing algorithm used to represent the datum being time-stamped;

b) the accuracy of the time in the time-stamps with respect to UTC;

c) any limitations on the use of the time-stamping service;

d) the subscriber's obligations as defined in clause 6.5.2, if any;

e) the relying party's obligations as defined in clause 6.6;

f) information on how to verify the time-stamp such that the relying party is considered to "reasonably rely" on the time-stamp (see clause 6.6) and any possible limitations on the validity period; and

g) any claim to meet the requirements on time-stamping services under national law.

The TSA should include in its time-stamping disclosure statement availability of its service.

EXAMPLE: Expected mean time between failure of the time-stamping service, expected mean time to recovery following a failure and provisions made for disaster recovery including back-up services.

The model TSA disclosure statement given in annex B may be used. Alternatively this may be provided as part of a subscriber / relying party agreement.

The TSA disclosure statement may be included in a TSA practice statement provided that it is conspicuous to the reader.

6.3 Terms and conditions

The general obligations specified in ETSI EN 319 401 [4], clause 6.2 shall apply.

6.4 Information security policy

The requirements identified in ETSI EN 319 401 [4], clause 6.3 shall apply.

6.5 TSA obligations

6.5.1 General

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

6.5.2 TSA obligations towards subscribers

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

6.6 Information for relying parties

The terms and conditions made available to relying parties (see clause 6.3) shall include an obligation on the relying party, when relying on a time-stamp, to:

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

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

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

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

7 TSA management and operation

7.1 Introduction

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

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

NOTE: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a TSA can employ in issuing time-stamps. In ETSI EN 319 401 [4], reference is made to other more general standards which can be used as a source of more detailed control requirements. Due to these factors the specificity of the requirements given under a given topic can vary.

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

7.2 Internal organization

The requirements identified in ETSI EN 319 401 [4], clause 7.1 shall apply. In addition the following particular requirements apply:

a) The TSA shall be a legal entity according to national law.

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

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

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

7.3 Personnel security

The requirements identified in ETSI EN 319 401 [4], clause 7.2 shall apply.

7.4 Asset management

The requirements identified in ETSI EN 319 401 [4], clause 7.3 shall apply.

7.5 Access control

The requirements identified in ETSI EN 319 401 [4], clause 7.4 shall apply.

7.6 Cryptographic controls

7.6.1 General

The requirements identified in ETSI EN 319 401 [4], clause 7.5 shall apply.

7.6.2 TSU key generation

The following particular requirements apply:

a) The generation of the TSU's signing key(s) shall be undertaken in a physically secured environment (as per clause 7.8) by personnel in trusted roles (as per clause 7.3) under, at least, dual control. The personnel authorized to carry out this function shall be limited to those required to do so under the TSA's practices.

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

- meets the requirements identified in ISO/IEC 19790 [2], level 3 or higher; or

NOTE 1: Demonstrated conformance to FIPS PUB 140-2 [i.9], level 3 is considered as fulfillment of this requirement.

- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [3]; or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

NOTE 2: Standards specifying common criteria protection profiles for TSP cryptographic modules, in accordance with ISO 15408 [3], are currently under development within CEN as CEN EN 419 221-2 [i.14] or CEN EN 419 221-3 [i.15], CEN EN 419 221-4 [i.16],or CEN EN 419 221-5 [i.17].

c) The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps 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-stamps as issued by the TSA.

NOTE 3: See ETSI TS 119 312 [i.7] for guidance on signature algorithms and their parameters.

d) A TSU's signing key should not be imported into different cryptographic modules.

7.6.3 TSU private key protection

The TSU private keys shall remain confidential and their integrity shall be maintained with at least the following particular requirements:

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

- meets the requirements identified in ISO/IEC 19790 [2], level 3 or higher; or

NOTE 1: Demonstrated conformance to FIPS PUB 140-2 [i.9], level 3 is considered as fulfillment of this requirement.

- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [3], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

NOTE 2: Standards specifying common criteria protection profiles for TSP cryptographic modules, in accordance with ISO 15408 [3], are currently under development within CEN as CEN EN 419 221-2 [i.14] or CEN EN 419 221-3 [i.15], CEN EN 419 221-4 [i.16],or CEN EN 419 221-5 [i.17].

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 clause 7.8). The personnel authorized to carry out this function shall be limited to those required to do so under the TSA's practices.

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

NOTE 3: Additional requirement for private key protection may be defined in the future following on the agreement of a time-stamping protection profile to be CEN EN 419 231 [i.13].

7.6.4 TSU public key certificate

The TSA shall guarantee the integrity and authenticity of the TSU signature verification (public) keys with at least the following particular requirements:

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

b) The TSU signature verification (public) key certificate should be issued by a certification authority operating under ETSI EN 319 411-1 [i.11].

c) The TSU shall not issue time-stamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device.

When obtaining a signature verification (public key) certificate, the TSA should verify that this certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority).

7.6.5 Rekeying TSU's key

The life-time of TSU's certificate shall not be longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose (see clause 7.6.1c).

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

- Clause 7.14 requires that records concerning time-stamping services be held for a period of time as appropriate for at least 1 year after the expiration of the validity of the TSU's signing keys. The longer the validity period of the TSU certificates will be, the longer the size of the records to be kept will be.
- Should a TSU private key or certificate be compromised, the older the TSU certificate the more time-stamps will be affected.

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

7.6.6 Life cycle management of signing cryptographic hardware

The following particular requirements apply:

a) Time-stamp signing cryptographic hardware shall not be tampered with during shipment.

b) Time-stamp signing cryptographic hardware shall not be tampered with when and 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 clause 7.8).

d) TSU private signing keys stored on TSU cryptographic module shall be erased upon device retirement in a way that it is practically impossible to recover them.

7.6.7 End of TSU key life cycle

The TSA shall define an expiration date for TSU's keys.

This date shall not be longer than the end of validity of the associate public key certificate

This date should take into account the lifetime defined in ‘recommended key sizes versus time' from ETSI TS 119 312 [i.7].

However in order to be able to verify during a sufficient lapse of time the validity of the time-stamps, the validity of the TSU's signing key should be reduced.

EXAMPLE: Public key valid 4 years, and private key reduced to 1 year by using private key usage period.

The expiration date for TSU's keys may be defined when the TSU cryptographic module is initialized or by setting a private key usage period within the TSU's public key certificate.

The TSU private signing keys shall not be 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.

7.7 Time-stamping

7.7.1 Time-stamp issuance

Time-stamps shall conform to the time-stamp profile as defined in ETSI EN 319 422 [5].

The time-stamps shall be issued securely and shall include the correct time.

In particular:

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

NOTE 1: The Bureau International des Poids et Mesures (BIPM) computes UTC on the basis of its local representations UTC(k) from a large ensemble of atomic clocks in national metrology institutes and national astronomical observatories round the world. The BIPM disseminates UTC through its monthly Circular T [i.6] (list 1). This is available on the BIPM website (www.bipm.org) and it officially identifies all those institutes having recognized UTC(k) time scales.

b) The time included in the time-stamp shall be synchronized with UTC [1] within the accuracy defined in the policy and, if present, within the accuracy defined in the time-stamp itself.

c) If the time-stamp provider's clock is detected (see clause 7.7.2 c) as being out of the stated accuracy (see clause 7.7.1 b) then time-stamps shall not be issued.

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

e) The time-stamp generation system shall reject any attempt to issue time-stamps if the signing private key has expired.

7.7.2 Clock synchronization with UTC

The TSA clock shall be synchronized with UTC [1] within the declared accuracy with at least the following particular requirements:

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

b) The declared accuracy shall be of 1 second or better.

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

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

d) The TSA shall detect if the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC.

NOTE 2: See clause 7.12 for notification requirements of such events to relying parties.

e) If it is detected that the time indicated in a time-stamp drifts or jumps out of synchronization with UTC, the TSU shall stop time-stamp issuance.

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

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

7.8 Physical and environmental security

The requirements identified in ETSI EN 319 401 [4], clause 7.6 shall apply. In addition the following particular requirements apply:

a) Access controls shall be applied to the cryptographic module to meet the requirements of security of cryptographic modules as identified in clause 7.6.

b) The following additional controls apply to time-stamping management:

- The time-stamping management facilities shall be operated in an environment which physically and logically protects the services from compromise through unauthorized access to systems or data.
- Every entry to the physically secure area shall be subject to independent oversight and non-authorised person shall be accompanied by an authorised person whilst in the secure area. Every entry and exist shall be logged.
- 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 protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The TSA's physical and environmental security policy for systems concerned with time-stamping management shall address as a minimum the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.
- Controls shall protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization.

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

7.9 Operation security

The requirements identified in ETSI EN 319 401 [4], clause 7.7 shall apply. In addition the following particular requirements apply:

System Planning

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

7.10 Network security

The requirements identified in ETSI EN 319 401 [4], clause 7.8 shall apply. In addition, the following particular requirements apply:

a) The TSA shall maintain and protect all TSU systems in a secure zone.

b) The TSA shall configure all TSU systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the TSA's operations.

c) Only trusted roles shall access secure zones and high security zones.

7.11 Incident management

The requirements identified in ETSI EN 319 401 [4], clause 7.9 shall apply.

7.12 Collection of evidence

The requirements identified in ETSI EN 319 401 [4], clause 7.10 shall apply. In addition the following particular requirements apply:

TSU key management

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

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

Clock Synchronization

c) 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 used in time-stamping.

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

7.13 Business continuity management

The requirements identified in ETSI EN 319 401 [4], clause 7.11 shall apply. In addition the following particular requirements apply:

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-stamps which have been issued.

b) In the case of a compromise, or suspected compromise or loss of calibration when issuing time-stamp 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-stamps until steps are taken to recover from the compromise.

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

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

7.14 TSA termination and termination plans

The requirements identified in ETSI EN 319 401 [4], clause 7.12 shall apply. In addition the following particular requirements apply:

a) When the TSA terminates its services, the TSA shall revoke the TSU's certificates.

7.15 Compliance

The requirements identified in ETSI EN 319 401 [4], clause 7.12 shall apply.

8 Additional requirements for Regulation (EU) No 910/2014

8.1 TSU public key certificate

When a time-stamp is claimed to be a qualified electronic time-stamp as per Regulation (EU) No 910/2014 [i.4], the TSU signature verification (public) key certificate should be issued by a certification authority operating under ETSI EN 319 411-2 [i.12] certificate policy.

NOTE 1: ETSI EN 319 411-2 [i.12] incorporates requirements from ETSI EN 319 411-1 [i.11].

NOTE 2: The relying party is expected to use a Trusted List to establish whether the time-stamp unit and the time-stamp are qualified. If the public key of the TSU is listed in the Trusted List and the service it represents is a qualified time-stamping service, then the time-stamps issued by this TSU can be considered as qualified. The qcStatement "`esi4-qtstStatement-1`" as defined in ETSI EN 319 422 [5], clause 9.1 can be used as an indication that the TSP claims the time-stamp to be a qualified electronic time-stamp.

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

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

Where consumers are involved, statutory protections can also apply - especially the Unfair Contract Terms Directive (Directive 93/13/EEC [i.5]) and the corresponding national implementations, which can even increase the level of protection.

These rules can constrain the TSA's capability to limit its liability, because the Directive 93/13/EEC [i.5] prohibits terms that have not been individually negotiated which cause a significant imbalance in the parties' rights and obligations to the detriment of the consumer.

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

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

Annex B (informative): Model TSA disclosure statement

B.1 Introduction

The proposed model TSA disclosure statement in table B.1 is designed for use by a TSP issuing time-stamps as a supplemental instrument of disclosure and notice. A TSA disclosure statement can assist a TSA to respond to regulatory requirements and concerns, particularly those related to consumer deployment. Further, the aim of the model TSA disclosure statement is to foster industry "self-regulation" and build consensus on those elements of a security policy and/or practice statement that require emphasis and disclosure.

Although security policy and practice statement documents are essential for describing and governing time-stamp policies and practices, many TSA users, especially consumers, can find these documents difficult to understand.

Consequently, there is a need for a supplemental and simplified instrument that can assist TSA users in making informed trust decisions. Consequently, a TSA disclosure statement is not intended to replace a security policy or practice statement.

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

B.2 TSA disclosure statement structure

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

Table B.1: Model of TSA disclosure statement structure

Statement types	Statement descriptions	Specific requirements
Entire agreement	A statement indicating that the disclosure statement is not the entire agreement, but only a part of it.	-
TSA contact info	The name, location and relevant contact information for the TSA.	-
Electronic time-stamp types and usage	A description of each class/type of electronic time-stamps issued by the TSA (in accordance with each time-stamp policy) and any restrictions on time-stamp usage.	Indication of the policy being applied (i.e. BTSP), including the contexts for which the time-stamp can be used (e.g. only for use with electronic signatures), the hashing algorithms, the expected life time of the time-stamp signature, any limitations on the use of the time-stamp and information on how to verify the time-stamp.
Reliance limits	The reliance limits, if any.	Indication of the accuracy of the time in the time-stamp, and the period of time for which TSA event logs (see clause 7.14) are maintained (and hence are available to provide supporting evidence).
Obligations of subscribers	The description of, or reference to, the critical subscriber obligations.	No specific requirements identified in the present document. Where applicable the TSA may specify additional obligations.
TSU public key certificate status checking obligations of relying parties	The extent to which relying parties are obligated to check the TSU public key certificate status, and references to further explanation.	Information on how to validate the TSU public key certificate status, including requirements to check the revocation status of TSU public key certificate, such that the relying party is considered to "reasonably rely" on the time-stamp (see clause 6.6).
Limited warranty and disclaimer/Limitation of liability	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	Limitations of liability (see annex A).
Applicable agreements and practice statement	Identification and references to applicable agreements, practice statement, time-stamp policy and other relevant documents.	-
Privacy policy	A description of and reference to the applicable privacy policy.	-
Refund policy	A description of and reference to the applicable refund policy.	-
Applicable law, complaints and dispute resolution	Statement of the choice of law, complaints procedure and dispute resolution mechanisms.	The procedures for complaints and dispute settlements. The applicable legal system.
TSA and repository licenses, trust marks, and audit	Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm.	If the TSA has been assessed to be conformant with the identified time-stamp policy, and if so through which independent party.

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

UTC is the time-scale maintained by the BIPM, with assistance from the IERS, which forms the basis of a coordinated dissemination of standard frequencies and time signals. It corresponds exactly in rate with TAI but differs from it by an integer number of seconds.

The full definition of UTC is contained in Recommendation ITU-R TF.460-6 [1].

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

Usually, a time-stamp becomes unverifiable beyond the end of the validity period of the certificate from the TSU, because the CA that has issued the certificate does not usually warrant any more providing revocation status information for expired certificates.

If at the time of verification:

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

then verification of a time-stamp can still be performed beyond the end of the validity period of the certificate from the TSU.

The validity may be maintained by applying an additional time-stamp to protect the integrity of the previous one. Alternatively the time-stamped data may be placed in secure storage.

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

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

Table E.1 identifies how the security controls objectives and other parts of the Best practices Time-Stamp Policy (BTSP) defined in the present document address the requirements of TSAs issuing qualified electronic time-stamps as defined in article 42 of the Regulation (EU) No 910/2014 [i.4].

Table E.1: Regulation (EU) No 910/2014 and qualified electronic time-stamp policy cross-reference

reference	Regulation (EU) No 910/2014 requirement	time-stamp policy reference
Article 3 Clause 33	*'electronic time stamp' means data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time*	7.7.1 Time-stamp issuance Time-stamp profiled in ETSI EN 319 422 [5]
Article 24 Clause 2	Requirements on qualified trust service provider providing qualified trust services	met, as relevant to time-stamping, through use of ETSI EN 319 401 [4]
Article 42 Clause 1 (a)	*it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably*	7.7.1 Time-stamp issuance items d & e
Article 42 Clause 1 (b)	*it is based on an accurate time source linked to Coordinated Universal Time* (UTC)	7.7.1 Time-stamp issuance items a, b & c
Article 42 Clause 1 (c)	*it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method*.	7.7.1 Time-stamp issuance Time-stamp profiled in ETSI EN 319 422 [5] requires an advanced electronic signature or seal

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

F.1 Managed time-stamping service

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

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

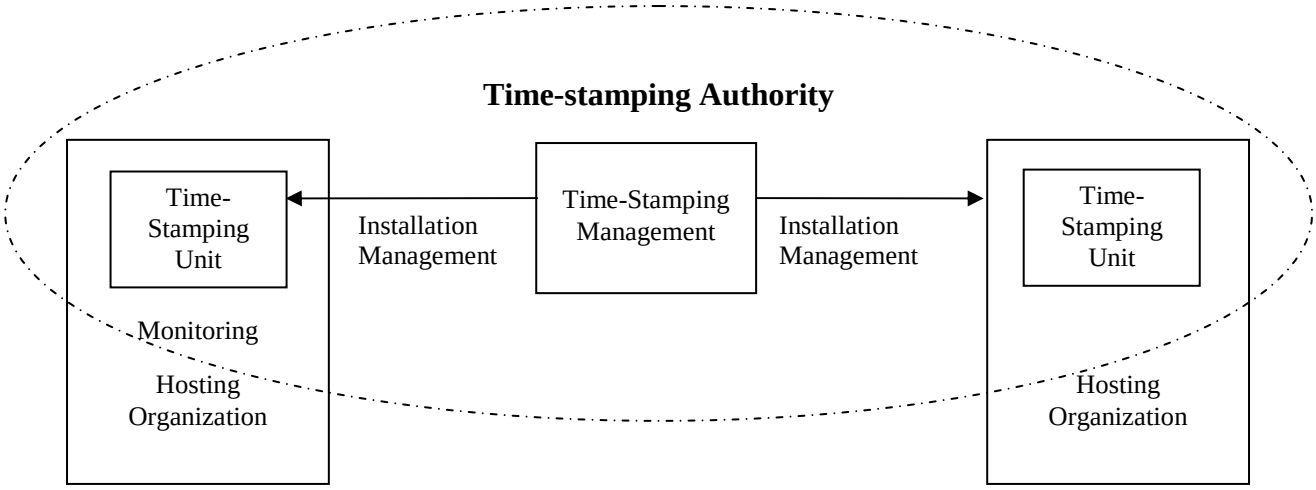

Figure F.1: Managed time-stamping service

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

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

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

F.2 Selective alternative quality

Some relying parties will be willing to take advantage of particular characteristics from a time-stamp such as a specific signature algorithm and/or key length or a specific accuracy for the time contained in the time-stamp.

These parameters can be considered as specifying a "quality" for the time-stamp.

Time-stamps with various qualities can be issued by different time-stamping units operated by the same or different TSAs.

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

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

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

General TSP policy (ETSI EN 319 401 [4]) requirements referenced.

Clause 3.1 Definitions, subscriber's definition.

Clause 6.2 Trust Service Practice Statement, updated disclosure statement.

Clause 7.6.2 TSU key generation, requirement b) updated to ISO a CEN/TS references.

Clause 7.6.2 TSU key generation, requirement d) recommending that same key should not be imported to multiple modules.

Clause 7.6.3 TSU private key protection, requirement a) updated to ISO a CEN/TS references.

Clause 7.6.4 TSU public key certificate, requirement c) added to disallow time-stamp issuance before a TSA certificate is loaded.

Clause 7.6.5 Rekeying TSU's key, note 1 reworded.

Clause 7.6.7 End of TSU key life cycle, added §1,§2 & §3.

Clause 7.7.2 Clock Synchronization with UTC, inserted requirement d) about drifts or jumps out of synchronization.

Annex H (informative): Conformity Assessment Check list

A check list for the policy requirements specified in the present document as well as the generic requirements which are independent of the TSP (as expressed in ETSI EN 319 401 [4]) is contained in the spreadsheet file which accompanies the present document (en_319421v010000a0.zip).

The checklist summarises the requirements in such a way that it can be used by the TSP itself to prepare for an assessment of its practices against the present document (i.e. serve as a basis for a self-declaration) and/or by the assessor when conducting the assessment, for the sake of facility for both the assessor and the TSP to be assessed.

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the check list file identified in this annex so that it can be used for its intended purposes and may further publish the completed check list.

History

Document history		
V1.1.1	April 2002	Publication as TS 102 023
V1.2.1	January 2003	Publication as TS 102 023
V1.2.2	October 2008	Publication as TS 102 023
V1.0.0	June 2015	EN Approval Procedure AP 20151016: 2015-06-18 to 2015-10-16