SLOVENSKI STANDARD
oSIST prEN 319 421 V1.2.0:2023

01-april-2023

Elektronski podpisi in infrastruktura (ESI) - Zahteve politike in varnosti za ponudnike storitev zaupanja, ki izdajajo časovne žige

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

Ta slovenski standard je istoveten z: **ETSI EN 319 421 V1.2.0 (2023-01)**

ICS:

35.030	Informacijska varnost	IT Security
35.040.01	Kodiranje informacij na splošno	Information coding in general

oSIST prEN 319 421 V1.2.0:2023 **en**

Draft ETSI EN 319 421 V1.2.0 (2023-01)

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

Reference
REN/ESI-0019421v1.2.1

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

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 is derived from the requirements specified in 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):	6 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].

The present document does not specify how the requirements identified can be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE 2: See ETSI EN 319 403-1 [i.9] for guidance on assessment of TSP's processes and services.

NOTE 3: The present document references ETSI EN 319 401 [4] for general policy requirements common to all classes of TSP's services.

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 https://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.

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

[2] ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".

[3] ISO/IEC 15408 (parts 1 to 3): "Information security, cybersecurity and privacy protection -- 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 token profiles".

[6] FIPS PUB 140-2 (2002): "Security Requirements for Cryptographic Modules".

[7] FIPS PUB 140-3 (2019): "Security Requirements for Cryptographic Modules".

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 319 122-1: "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 https://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] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.10] 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.11] 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.12] EN 419231: "Protection profile for trustworthy systems supporting time stamping", (produced by CEN).

[i.13] TS 419221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup", (produced by CEN).

[i.14] TS 419221-3: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services", (produced by CEN).

[i.15] TS 419221-4: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup", (produced by CEN).

[i.16] EN 419221-5: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services", (produced by CEN).

[i.17] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

3 Definitions of terms, symbols, abbreviations and notation

3.1 Terms

For the purposes of the present document, the terms 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].

Time-Stamping Authority (TSA): TSP providing time-stamping services using one or more time-stamping units

time-stamping service: trust service for issuing time-stamps

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

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

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

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 (https://www.bipm.org/).

3.2 Symbols

Void.

3.3 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
IERS	International Earth Rotation and Reference System Service
IT	Information Technology
TAI	International Atomic Time
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

3.4 Notation

The requirements identified in the present document include:

a) Requirements applicable to any policy. Such requirements are indicated by clauses without any additional marking.

b) Requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]".

c) Requirements that include several choices which ought to be selected according to the applicable situation. Such requirements are indicated by clauses marked by "[CHOICE]".

Each requirement is identified as follows:

<3 letters service component> - < the clause number> - <2 digit number - incremental>.

The service components are:

- **OVR:** General requirement (requirement applicable to more than 1 component)
- **TIS:** Time-stamp Issuance Services

The management of the requirement identifiers for subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish new requirements.
- The requirement identifier for deleted requirements are left and completed with "Void".
- The requirement identifier for modified requirement are left void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

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.