ICS 35.240.30 SLOVENSKÁ TECHNICKÁ NORMA Február 2017

STN

Elektronické podpisy a infraštruktúry (ESI). Požiadavky politiky a bezpečnostné požiadavky pre poskytovateľov dôveryhodných služieb vydávajúcich časové pečiatky.

STN
EN 319 421 V1.1.1

87 9421

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 01/17

Obsahuje: EN 319 421 V1.1.1:2016

124183

ETSI EN 319 421 V1.1.1 (2016-03)

EUROPEAN STANDARD

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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

National transposition dates	
Date of adoption of this EN:	22 February 2016
Date of latest announcement of this EN (doa):	31 May 2016
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 November 2016
Date of withdrawal of any conflicting National Standard (dow):	30 June 2017

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.9].

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.

[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 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 token profiles".

[6] FIPS PUB 140-2 (2001): "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 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] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - 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] CEN EN 419 231: "Protection profile for trustworthy systems supporting time stamping".

[i.13] CEN EN 419 221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup".

[i.14] CEN EN 419 221-3: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for Cryptographic module for CSP key generation services".

[i.15] CEN EN 419 221-4: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup".

[i.16] CEN EN 419 221-5: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services".