ICS 35.240.30 SLOVENSKÁ TECHNICKÁ NORMA Október 2021

STN	Elektronické podpisy a infraštruktúry (ESI) Požiadavky politiky a bezpečnosti na poskytovateľov dôveryhodných služieb vydávajúcich certifikáty Časť 1: Obecné požiadavky	STN EN 319 411-1 V1.3.1 87 9411

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

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. 09/21

Obsahuje: EN 319 411-1 V1.3.1:2021

133672

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2021

ETSI EN 319 411-1 V1.3.1 (2021-05)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

Reference

REN/ESI-0019411-1v131

Keywords

e-commerce, electronic signature, extended validation certificate, public key, security, 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

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 1 of a multi-part deliverable covering the Policy and security requirements for Trust Service Providers issuing certificates, as identified below:

ETSI EN 319 411-1: "General requirements";

ETSI EN 319 411-2: "Requirements for trust service providers issuing EU qualified certificates";

ETSI TR 119 411-4: "Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2 [i.5]".

NOTE: Part 3 of this multi-part deliverable has been withdrawn.

The present document is derived from the requirements specified in ETSI TS 102 042 [i.6].

National transposition dates	
Date of adoption of this EN:	12 May 2021
Date of latest announcement of this EN (doa):	31 August 2021
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	28 February 2022
Date of withdrawal of any conflicting National Standard (dow):	28 February 2022

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

Electronic commerce, in its broadest sense, is a way of doing business and communicating across public and private networks. An important requirement of electronic commerce is the ability to identify the originator and protect the confidentiality of electronic exchanges. This is commonly achieved by using cryptographic mechanisms which are supported by a Trust Service Provider (TSP) issuing certificates, commonly called a Certification Authority (CA).

For participants of electronic commerce to have confidence in the security of these cryptographic mechanisms they need to have confidence that the TSP has properly established procedures and protective measure in order to minimize the operational and financial threats and risks associated with public key cryptographic systems.

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.14] and those from CA/Browser Forum, BRG [5].

Bodies wishing to establish policy requirements for TSPs issuing certificates in a regulatory context other than the EU can base their requirements on those specified in the present document and specify any additional requirements in a manner similar to ETSI EN 319 411-2 [i.5], which builds on the present document requirements so as to benefit from the use of generally accepted global best practices.

1 Scope

The present document specifies generally applicable policy and security requirements for Trust Service Providers (TSPs) issuing public key certificates, including trusted web site certificates.

The policy and security requirements are defined in terms of requirements for the issuance, maintenance and life-cycle management of certificates. These policy and security requirements support several reference certificate policies, defined in clauses 4 and 5.

A framework for the definition of policy requirements for TSPs issuing certificates in a specific context where particular requirements apply is defined in clause 7.

The present document covers requirements for CA hierarchies, however this is limited to supporting the policies as specified in the present document. It does not include requirements for root CAs and intermediate CAs for other purposes.

The present document is applicable to:

- the general requirements of certification in support of cryptographic mechanisms, including digital signatures for electronic signatures and seals;
- the general requirements of certification authorities issuing TLS/SSL certificates;
- the general requirements of the use of cryptography for authentication and encryption.

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: See ETSI EN 319 403 [i.2] for guidance on assessment of TSP's processes and services. The present document references ETSI EN 319 401 [8] for general policy requirements common to all classes of TSP's services.

The present document includes provisions consistent with the requirements from the CA/Browser Forum in EVCG [4] and BRG [5].

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

[2] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".

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

[4] CA/Browser Forum (V1.6.7): "Guidelines for The Issuance and Management of Extended Validation Certificates".

[5] CA/Browser Forum (V1.7.1): "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates".

[6] ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks".

[7] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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

[9] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

[10] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

[11] IETF RFC 6960: "X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP".

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

[13] ETSI TS 119 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

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] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.2] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.3] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[i.4] ISO 19005 (parts 1 to 3): "Document management - electronic document file format for long-term preservation".

[i.5] 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.6] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[i.7] ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security management".

[i.8] ISO/IEC 7498-2/Recommendation ITU-T X.800: "Data communications network - Open systems interconnection - Security, structure and applications: Security architecture for open systems interconnection for CCITT applications".

[i.9] TS 419 261: "Security requirements for trustworthy systems managing certificates and time stamps", (produced by CEN).

[i.10] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.11] IETF RFC 5246: "The Transport Layer Security Protocol Version 1.2".

[i.12] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.13] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.14] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.15] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.16] TS 419 221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup", (produced by CEN).

[i.17] TS 419 221-3: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for Cryptographic module for CSP key generation services", (produced by CEN).

[i.18] TS 419 221-4: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup", (produced by CEN).

[i.19] EN 419 221-5: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services", (produced by CEN).

[i.20] ETSI TR 119 411-4: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2".

[i.21] ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".

[i.22] ETSI TS 119 511:"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".