



SLOVENSKI STANDARD
SIST EN 319 411-1 V1.5.1:2025

01-junij-2025

Elektronski podpisi in infrastrukture zaupanja (ESI) - Zahteve politike in varnosti za ponudnike storitev zaupanja, ki izdajajo digitalna potrdila - 1. del: Splošne zahteve

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

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

Ta slovenski standard je istoveten z: ETSI EN 319 411-1 V1.5.1 (2025-04)

SIST EN 319 411-1 V1.5.1:2025

<https://standards.iteh.ai/catalog/standards/sist/cb578481-de9b-4165-8f65-9e06e492a899/sist-en-319-411-1-v1-5-1-2025>

ICS:

03.080.99	Druge storitve	Other services
35.030	Informacijska varnost	IT Security
35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST EN 319 411-1 V1.5.1:2025

en

ETSI EN 319 411-1 V1.5.1 (2025-04)



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

[SIST EN 319 411-1 V1.5.1:2025](https://standards.iteh.ai/catalog/standards/sist/cb578481-de9b-4165-8f65-9e06e492a899/sist-en-319-411-1-v1-5-1-2025)

<https://standards.iteh.ai/catalog/standards/sist/cb578481-de9b-4165-8f65-9e06e492a899/sist-en-319-411-1-v1-5-1-2025>

Reference

REN/ESI-0019411-1v151

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 the
[ETSI Search & Browse Standards](#) application.

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 on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2025.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	6
Introduction	6
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	8
3 Definition of terms, symbols, abbreviations and notations	10
3.1 Terms.....	10
3.2 Symbols.....	12
3.3 Abbreviations	12
3.4 Notations	13
4 General concepts	14
4.1 General policy requirements concepts.....	14
4.2 Certification Services applicable documentation	14
4.2.1 Certification Practice Statement	14
4.2.2 Certificate Policy	14
4.2.3 Terms and conditions and PKI disclosure statement	16
4.3 Certification services	16
5 General provisions on Certification Practice Statement and Certificate Policies.....	17
5.1 General requirements	17
5.2 Certification Practice Statement requirements	18
5.3 Certificate Policy name and identification	19
5.4 PKI participants.....	20
5.4.1 Certification Authority.....	20
5.4.2 Subscriber and subject	20
5.4.3 Others.....	21
5.5 Certificate usage	21
6 Trust Service Providers practice.....	21
6.1 Publication and repository responsibilities.....	21
6.2 Identification and authentication.....	22
6.2.1 Naming	22
6.2.2 Initial identity validation.....	22
6.2.3 Identification and authentication for Re-key requests	27
6.2.4 Identification and authentication for revocation requests	27
6.3 Certificate Life-Cycle operational requirements	28
6.3.1 Certificate application.....	28
6.3.2 Certificate application processing.....	28
6.3.3 Certificate issuance	29
6.3.4 Certificate acceptance	31
6.3.5 Key pair and certificate usage.....	32
6.3.6 Certificate renewal	34
6.3.7 Certificate Re-key.....	34
6.3.8 Certificate modification	35
6.3.9 Certificate revocation and suspension.....	35
6.3.10 Certificate status services.....	37
6.3.11 End of subscription	38
6.3.12 Key escrow and recovery.....	38
6.4 Facility, management, and operational controls.....	38
6.4.1 General.....	38
6.4.2 Physical security controls	38

6.4.3	Procedural controls	39
6.4.4	Personnel controls.....	39
6.4.5	Audit logging procedures.....	39
6.4.6	Records archival	40
6.4.7	Key changeover	40
6.4.8	Compromise and disaster recovery	41
6.4.9	Certification Authority or Registration Authority termination	42
6.5	Technical security controls	42
6.5.1	Key pair generation and installation	42
6.5.2	Private key protection and cryptographic module engineering controls	45
6.5.3	Other aspects of key pair management	45
6.5.4	Activation data	46
6.5.5	Computer security controls	46
6.5.6	Life cycle security controls.....	47
6.5.7	Network security controls.....	47
6.5.8	Timestamping	47
6.6	Certificate, CRL and OCSP profiles.....	47
6.6.1	Certificate profile	47
6.6.2	CRL profile	48
6.6.3	OCSP profile.....	48
6.7	Compliance audit and other assessment	48
6.8	Other business and legal matters	49
6.8.1	Fees	49
6.8.2	Financial responsibility	49
6.8.3	Confidentiality of business information.....	49
6.8.4	Privacy of personal information.....	49
6.8.5	Intellectual property rights	49
6.8.6	Representations and warranties.....	49
6.8.7	Disclaimers of warranties	50
6.8.8	Limitations of liability	50
6.8.9	Indemnities	50
6.8.10	Term and termination.....	50
6.8.11	Individual notices and communications with participants	50
6.8.12	Amendments	50
6.8.13	Dispute resolution procedures.....	50
6.8.14	Governing law	50
6.8.15	Compliance with applicable law	50
6.8.16	Miscellaneous provisions.....	50
6.9	Other provisions	50
6.9.1	Organizational.....	50
6.9.2	Additional testing.....	51
6.9.3	Disabilities	51
6.9.4	Terms and conditions.....	51
7	Framework for the definition of other certificate policies.....	52
7.1	Certificate policy management.....	52
7.2	Additional requirements	52
Annex A (informative):	Model PKI disclosure statement.....	53
A.1	Introduction	53
A.2	The PDS structure	53
A.3	The PDS format.....	54
Annex B (informative):	Conformity assessment checklist.....	55
Annex C (informative):	Bibliography.....	56
Annex D (informative):	Change history	57
History		60

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 IPR online database](#).

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™**, **LTE™** and **5G™** logo 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 Trust 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";

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

ETSI TR 119 411-4: "Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2";

ETSI TS 119 411-5: "Implementation of qualified certificates for website authentication as in amended regulation 910/2014";

ETSI TS 119 411-6: "Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates".

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