



SLOVENSKI STANDARD

SIST EN 319 411-2 V2.5.1:2023

01-december-2023

Elektronski podpisi in infrastruktura (ESI) - Zahteve politike in varnosti za ponudnike storitev zaupanja, ki izdajajo digitalna potrdila - 2. del: Zahteve za ponudnike storitev zaupanja, ki izdajajo kvalificirana digitalna potrdila v EU

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

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

Ta slovenski standard je istoveten z: ETSI EN 319 411-2 V2.5.1 (2023-10)

[SIST EN 319 411-2 V2.5.1:2023](https://standards.iteh.ai/catalog/standards/sist/795689a0-3032-45c5-9d83-8efa7dc4d6c5/sist-en-319-411-2-v2-5-1-2023)

<https://standards.iteh.ai/catalog/standards/sist/795689a0-3032-45c5-9d83-8efa7dc4d6c5/sist-en-319-411-2-v2-5-1-2023>

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 319 411-2 V2.5.1:2023 en

ETSI EN 319 411-2 V2.5.1 (2023-10)



**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**

[SIST EN 319 411-2 V2.5.1:2023](https://standards.iteh.ai/catalog/standards/sist/795689a0-3032-45c5-9d83-8efa7dc4d6c5/sist-en-319-411-2-v2-5-1-2023)

<https://standards.iteh.ai/catalog/standards/sist/795689a0-3032-45c5-9d83-8efa7dc4d6c5/sist-en-319-411-2-v2-5-1-2023>

Reference

REN/ESI-0019411-2v251

Keywords

e-commerce, electronic signature, security, trust services

ETSI650 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:

<https://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/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

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 2023.
All rights reserved.

Contents

Intellectual Property Rights	6
Foreword.....	6
Modal verbs terminology.....	6
Introduction	7
1 Scope	8
2 References	8
2.1 Normative references	8
2.2 Informative references.....	8
3 Definition of terms, symbols, abbreviations and notations	9
3.1 Terms.....	9
3.2 Symbols.....	9
3.3 Abbreviations	10
3.4 Notations	10
4 General concepts	11
4.1 General policy requirements concepts.....	11
4.2 Certificate policy and certification practice statement	11
4.2.1 Overview	11
4.2.2 Purpose	11
4.2.3 Level of specificity	11
4.2.4 Approach	11
4.2.5 Certificate policy	11
4.3 Other TSP statements	13
4.4 Certification services.....	13
5 General provisions on Certification Practice Statement and Certificate Policies.....	13
5.1 General requirements	13
5.2 Certification Practice Statement Requirements.....	14
5.3 Certificate Policy name and identification	14
5.4 PKI Participants.....	15
5.4.1 Certification authority.....	15
5.4.2 Subscriber and subject	15
5.4.3 Others.....	15
5.5 Certificate Usage	15
5.5.1 QCP-n	15
5.5.2 QCP-l.....	15
5.5.3 QCP-n-qscd.....	15
5.5.4 QCP-l-qscd	15
5.5.5 QEVCP-w	15
5.5.6 QNCP-w	15
5.5.7 QNCP-w-gen	16
6 Trust Service Providers practice.....	16
6.1 Publication and Repository Responsibilities	16
6.2 Identification and Authentication	16
6.2.1 Naming	16
6.2.2 Initial Identity Validation.....	16
6.2.3 Identification and authentication for Re-key requests	17
6.2.4 Identification and authentication for revocation requests	17
6.3 Certificate Life-Cycle Operational Requirements	17
6.3.1 Certificate Application.....	17
6.3.2 Certificate application processing.....	17
6.3.3 Certificate issuance	17
6.3.4 Certificate acceptance	17
6.3.5 Key Pair and Certificate Usage.....	17
6.3.6 Certificate Renewal.....	18

6.3.7	Certificate Re-key	18
6.3.8	Certificate Modification	18
6.3.9	Certificate Revocation and Suspension	18
6.3.10	Certificate Status Services	18
6.3.11	End of Subscription	20
6.3.12	Key Escrow and Recovery	20
6.4	Facility, Management and Operational Controls	20
6.4.1	General	20
6.4.2	Physical Security Controls	20
6.4.3	Procedural Controls	20
6.4.4	Personnel Controls	20
6.4.5	Audit Logging Procedures	20
6.4.6	Records Archival	20
6.4.7	Key Changeover	21
6.4.8	Compromise and Disaster Recovery	21
6.4.9	CA or RA Termination	21
6.5	Technical Security Controls	21
6.5.1	Key Pair Generation and Installation	21
6.5.2	Private Key Protection and Cryptographic Module Engineering Controls	22
6.5.3	Other Aspects of Key Pair Management	22
6.5.4	Activation Data	22
6.5.5	Computer Security Controls	22
6.5.6	Life Cycle Security Controls	22
6.5.7	Network Security Controls	22
6.5.8	Time-stamping	22
6.6	Certificate, CRL, and OCSP Profiles	22
6.6.1	Certificate Profile	22
6.6.2	CRL Profile	23
6.6.3	OCSP Profile	23
6.7	Compliance Audit and Other Assessment	23
6.8	Other Business and Legal Matters	24
6.8.1	Fees	24
6.8.2	Financial Responsibility	24
6.8.3	Confidentiality of Business Information	24
6.8.4	Privacy of Personal Information	24
6.8.5	Intellectual Property Rights	24
6.8.6	Representations and Warranties	24
6.8.7	Disclaimers of Warranties	24
6.8.8	Limitations of Liability	24
6.8.9	Indemnities	24
6.8.10	Term and Termination	24
6.8.11	Individual notices and communications with participants	24
6.8.12	Amendments	25
6.8.13	Dispute Resolution Procedures	25
6.8.14	Governing Law	25
6.8.15	Compliance with Applicable Law	25
6.8.16	Miscellaneous Provisions	25
6.9	Other Provisions	25
6.9.1	Organizational	25
6.9.2	Additional testing	25
6.9.3	Disabilities	25
6.9.4	Terms and conditions	25
7	Framework for the definition of other certificate policies built on the present document	26
7.1	Certificate policy management	26
7.2	Additional requirements	26
Annex A (informative): Regulation and EU qualified certificate policy mapping		27
Annex B (informative): Conformity Assessment Checklist		31
Annex C (informative): Change history		32

History33

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

[SIST EN 319 411-2 V2.5.1:2023](https://standards.iteh.ai/catalog/standards/sist/795689a0-3032-45c5-9d83-8efa7dc4d6c5/sist-en-319-411-2-v2-5-1-2023)

<https://standards.iteh.ai/catalog/standards/sist/795689a0-3032-45c5-9d83-8efa7dc4d6c5/sist-en-319-411-2-v2-5-1-2023>

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 2 of a multi-part deliverable covering policy requirements for Trust Service Providers issuing certificates. Full details of the entire series can be found in part 1 [2].

The present document is derived from the requirements specified in ETSI TS 101 456 [i.2].

National transposition dates

Date of adoption of this EN:	4 October 2023
Date of latest announcement of this EN (doa):	31 January 2024
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 July 2024
Date of withdrawal of any conflicting National Standard (dow):	31 July 2024

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 Regulation (EU) No 910/2014 [i.1] establishes a legal framework for electronic signature and electronic seal and for website authentication services. These concepts can be commonly achieved by using cryptographic mechanisms. Electronic signatures and seals implemented by this way are digital signatures. Cryptographic mechanisms are generally supported by a Trust Service Provider (TSP) issuing public key certificates, commonly called a Certification Authority (CA).

By providing general policy and security requirements for trust service providers issuing certificates, the part 1 of the series ETSI EN 319 411-1 [2], is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, requirements from Regulation (EU) No 910/2014 [i.1] and from CA/Browser Forum documents BRG [i.3] and EVCG [i.7].

The present document incorporates the general policy and security requirements as specified in ETSI EN 319 411-1 [2] and adds further requirements in order to meet the specific requirements of Regulation (EU) N° 910/2014 for TSPs issuing EU qualified certificates for electronic signatures and/or EU qualified certificates for electronic seals and/or EU qualified certificates for website authentication in accordance with but not limited to Articles 19, 24, 28, 38 and 45 of Regulation (EU) No 910/2014 [i.1].

Bodies wishing to establish policy requirements for TSPs issuing certificates in a regulatory context other than the EU can build their specifications on the general policy requirements specified in ETSI EN 319 411-1 [2] to benefit from global best practices, and specify any additional requirements in a manner similar to the present document.

Conformance to the present document on its own does not imply that the TSP, nor the certificates issued by the TSP, are qualified in accordance with Regulation (EU) No 910/2014 [i.1].

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

[SIST EN 319 411-2 V2.5.1:2023](https://standards.iteh.ai/catalog/standards/sist/795689a0-3032-45c5-9d83-8efa7dc4d6c5/sist-en-319-411-2-v2-5-1-2023)

<https://standards.iteh.ai/catalog/standards/sist/795689a0-3032-45c5-9d83-8efa7dc4d6c5/sist-en-319-411-2-v2-5-1-2023>

1 Scope

The present document specifies policy and security requirements for the issuance, maintenance and life-cycle management of EU qualified certificates as defined in Regulation (EU) No 910/2014 [i.1]. These policy and security requirements support reference certificate policies for the issuance, maintenance and life-cycle management of EU qualified certificates issued to natural persons (including natural persons associated with a legal person or a website) and to legal persons (including legal persons associated with a website), respectively.

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.6] for guidance on assessment of TSP's processes and services. The present document references ETSI EN 319 411-1 [2] for general requirements on TSP issuing certificates.

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] [ETSI EN 319 401](#): "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- [2] [ETSI EN 319 411-1](#): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements".
- [3] [ETSI EN 319 412-5](#): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".
- [4] [ISO/IEC 9594-8/Recommendation ITU-T X.509](#): "Information technology - Open Systems Interconnection - Part 8: The Directory: Public-key and attribute certificate frameworks".

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] [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.2] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[i.3] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

NOTE: The version is as referenced in ETSI EN 319 411-1 [2].

[i.4] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.5] [Directive 95/46/EC](#) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.6] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.7] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

NOTE: The version is as referenced in ETSI EN 319 411-1 [2].

[i.8] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.9] IETF RFC 6960: "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[i.10] 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.11] [Commission implementing decision \(EU\) 2015/1505 of 8 September 2015](#) laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of 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.

[i.12] ETSI TS 119 615: "Electronic Signatures and Infrastructures (ESI); Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists".

[i.13] ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 401 [1], ETSI EN 319 411-1 [2], Regulation (EU) No 910/2014 [i.1] and the following apply:

EU Qualified Certificate: Qualified Certificate as specified in Regulation (EU) No 910/2014 [i.1].

Qualified electronic Signature/Seal Creation Device (QSCD): As specified in Regulation (EU) No 910/2014 [i.1].

3.2 Symbols

Void.