SLOVENSKI STANDARD
oSIST prEN 319 412-2 V2.1.3:2020

01-julij-2020

Elektronski podpisi in infrastruktura (ESI) - Profili potrdil - 2. del: Profil potrdil za potrdila, izdana fizičnim osebam

Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 319 412-2 V2.2.1:2020
https://standards.iteh.ai/catalog/standards/sist/f4524cbd-0307-4616-a6cd-0cebb12f744f/sist-en-319-412-2-v2-2-1-2020

Ta slovenski standard je istoveten z: **ETSI EN 319 412-2 V2.1.3 (2020-04)**

ICS:

03.080.99	Druge storitve	Other services
35.040.01	Kodiranje informacij na splošno	Information coding in general

oSIST prEN 319 412-2 V2.1.3:2020 **en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

oSIST prEN 319 412-2 V2.1.3:2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 319 412-2 V2.2.1:2020
https://standards.iteh.ai/catalog/standards/sist/f4524cbd-0307-4fd6-afad-0ecbb13f744f/sist-en-319-412-2-v2-2-1-2020

oSIST prEN 319 412-2 V2.1.3:2020

Draft ETSI EN 319 412-2 V2.1.3 (2020-04)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 319 412-2 V2.2.1:2020
https://standards.iteh.ai/catalog/standards/sist/f4524cbd-0307-4fd6-afad-0ecbb13f744f/sist-en-319-412-2-v2-2-1-2020

oSIST prEN 319 412-2 V2.1.3:2020

Reference
REN/ESI-0019412-2v221

Keywords
electronic signature, IP, profile, 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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Important notice

SIST EN 319 412-2 V2.2.1:2020
https://standards.iteh.ai/catalog/standards/sist/[illegible]-4fd6-afad-0ecbb13f744f/sist-en-319-412-2-v2-2-1-2020

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

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 2020.
All rights reserved.

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.

oSIST prEN 319 412-2 V2.1.3:2020

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 319 412-2 V2.2.1:2020
https://standards.iteh.ai/catalog/standards/sist/f4524cbd-0307-4fd6-afad-0ecbb13f744f/sist-en-319-412-2-v2-2-1-2020

oSIST prEN 319 412-2 V2.1.3:2020

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

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.

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 part 2 of multi-part deliverable covering the Certificates Profiles. Full details of the entire series can be found in part 1 [i.4].

The present document was previously published as ETSI TS 102 280 [i.8].

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 319 412-2 V2.2.1:2020
https://standards.iteh.ai/catalog/standards/sist/1452-4cbd-0307-4fd6-afad-0ecbb13f744f/sist-en-319-412-2-v2-2-1-2020

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

ITU and ISO issued standards for certification of public keys in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3] which are used for the security of communications and data for a wide range of electronic applications.

oSIST prEN 319 412-2 V2.1.3:2020

Regulation (EU) No 910/2014 [i.5] 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 defines requirements on specific types of certificates named "qualified certificates". Implementation of Directive 1999/93/EC [i.1] and deployment of certificate infrastructures throughout Europe as well as in countries outside of Europe, have resulted in a variety of certificate implementations for use in public and closed environments, where some are declared as qualified certificates while others are not.

Applications need support from standardized identity certificates profiles, in particular when applications are used for digital signatures, authentication and secure electronic exchange in open environments and international trust scenarios, but also when certificates are used in local application contexts.

This multi-part deliverable aims to maximize the interoperability of systems issuing and using certificates both in the European context under the Regulation (EU) No 910/2014 [i.5] and in the wider international environment.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 319 412-2 V2.2.1:2020
https://standards.iteh.ai/catalog/standards/sist/f4524cbd-0307-4fd6-afad-0ecbb13f744f/sist-en-319-412-2-v2-2-1-2020

oSIST prEN 319 412-2 V2.1.3:2020

1 Scope

The present document specifies requirements on the content of certificates issued to natural persons. This profile builds on IETF RFC 5280 [1] for generic profiling of Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3].

This profile supports the requirements of EU Qualified Certificates as specified in the Regulation (EU) No 910/2014 [i.5] as well as other forms of certificate. The scope of the present document is primary limited to facilitate interoperable processing and display of certificate information. This profile therefore excludes support for some certificate information content options, which can be perfectly valid in a local context but which are not regarded as relevant or suitable for use in widely deployed applications.

The present document focuses on requirements on certificate content. Requirements on decoding and processing rules are limited to aspects required to process certificate content defined in the present document. Further processing requirements are only specified for cases where it adds information that is necessary for the sake of interoperability.

Certain applications or protocols impose specific requirements on certificate content. The present document is based on the assumption that these requirements are adequately defined by the respective application or protocol. It is therefore outside the scope of the present document to specify such application or protocol specific certificate content.

2 References

2.1 Normative references

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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/.

SIST EN 319 412-2 V2.2.1:2020
https://standards.iteh.ai/catalog/standards/sist/[illegible]-en-319-412-2-v2-2-1-2020

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

[2] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[3] IETF RFC 7230 to IETF RFC 7235: "Hypertext Transfer Protocol -- HTTP/1.1".

[4] IETF RFC 4516: "Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator".

[5] IETF RFC 2818: "HTTP Over TLS".

[6] Recommendation ITU-T X.520 (10/2012): "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

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.

oSIST prEN 319 412-2 V2.1.3:2020

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

[i.3] Recommendation ITU-T X.509 | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.4] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

[i.5] 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.6] 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.7] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.8] ETSI TS 102 280: "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

3 Definition of terms, symbols and abbreviations

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 412-1 [i.4] apply.

SIST EN 319 412-2 V2.2.1:2020
https://standards.iteh.ai/catalog/standards/sist/f4524cbd-0307-4fd6-afad-0ecbb13f744f/sist-en-319-412-2-v2-2-1-2020

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certification Authority
CRL	Certificate Revocation List
EC	European Commission
EU	European Union
ISO	International Standards Organization
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
RFC	Request For Comments

4 General certificate profile requirements

4.1 Generic requirements

All certificate fields and extensions shall comply with IETF RFC 5280 [1] with the amendments specified in the present document.

oSIST prEN 319 412-2 V2.1.3:2020

Certificate extensions shall not be marked critical unless criticality is explicitly allowed or required in the present document or in IETF RFC 5280 [1].

4.2 Basic certificate fields

4.2.1 Version

The version shall be V3 (defined by the integer value 2).

4.2.2 Signature

Signature algorithm should be selected according to ETSI TS 119 312 [i.7].

NOTE: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.7] can be superseded by national recommendations.

4.2.3 Issuer

4.2.3.1 Legal person issuers

The identity of the issuer, when the issuer is a legal person, shall contain at least the following attributes as specified in Recommendation ITU-T X.520 [6]:

- `countryName`;
- `organizationName`; and
- `commonName`.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The identity of the issuer, when the issuer is a legal person, should contain the following attribute as specified in Recommendation ITU-T X.520 [6]:

https://standards.iteh.ai/catalog/standards/sist/f4524cbd-0307-4fd6-afad-0ecbb13f744f/sist-en-319-412-2-v2-2-1-2020

- `organizationIdentifier`.

Each attribute shall be limited to a single instance of the attribute. Additional attributes may be present.

The `countryName` attribute shall specify the country in which the issuer of the certificate is established.

The `organizationName` attribute shall contain the full registered name of the certificate issuing organization.

The `organizationIdentifier` attribute shall contain an identification of the certificate issuing organization different from the organization name.

The `commonName` attribute value shall contain a name commonly used by the subject to represent itself. This name need not be an exact match of the fully registered organization name.

NOTE: Earlier editions of Recommendation ITU-T X.520 [6] had size limitations on attribute content where e.g. `commonName` used to have a size limitation of 64 characters. The size limitations of attributes referenced in the present document (except `countryName`) are no longer present in the current edition of Recommendation ITU-T X.520 [6]. Interoperability issues can arise due to current implementations of Recommendation ITU-T X.520 [6] still operating in accordance with the previous size limitations.

4.2.3.2 Natural person issuers

The identity of the issuer, when the issuer is a natural person shall contain at least the following attributes as specified in Recommendation ITU-T X.520 [6]:

- `countryName`;
- choice of (`givenName` and `surname`) or `pseudonym`;