



SLOVENSKI STANDARD
SIST EN 319 412-2 V2.1.1:2016
01-maj-2016

Elektronski podpisi in infrastruktura (ESI) - Profili potrdil - 2. del: Profil potrdila za potrdila, ki se izdajajo 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)

Ta slovenski standard je istoveten z: **ETSI EN 319 412-2 V2.1.1 (2016-02)**

SIST EN 319 412-2 V2.1.1:2016
<https://standards.iteh.ai/catalog/standards/sist/128c809d-76af-4137-903f-7acae06d3311/sist-en-319-412-2-v2-1-1-2016>

ICS:

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

SIST EN 319 412-2 V2.1.1:2016 **en**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 319 412-2 V2.1.1:2016

<https://standards.iteh.ai/catalog/standards/sist/128c809d-7baf-4137-903f-7acae06d3311/sist-en-319-412-2-v2-1-1-2016>

ETSI EN 319 412-2 V2.1.1 (2016-02)



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

<https://standards.iteh.ai/catalog/standards/sist/128c809d-7baf-4137-903f-7acae06d3311/sist-en-319-412-2-v2-1-1-2016>

Reference

REN/ESI-0019412-2V211

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)

SIST EN 319 412-2 V2.1.1:2016

<https://standards.iteh.ai/catalog/standards/sist/128c809d-7baf-4137-903f-7acae06d3371/etsi-en-319-412-2-v2-1-1-2016> **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

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.

© European Telecommunications Standards Institute 2016.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definitions and abbreviations.....	7
3.1 Definitions	7
3.2 Abbreviations	7
4 General certificate profile requirements.....	7
4.1 Generic requirements	7
4.2 Basic certificate fields	7
4.2.1 Version.....	7
4.2.2 Signature	8
4.2.3 Issuer.....	8
4.2.3.1 Legal person issuers	8
4.2.3.2 Natural person issuers	8
4.2.4 Subject	9
4.2.5 Subject public key info	9
4.3 Standard certificate extensions.....	9
4.3.1 Authority key identifier	9
4.3.2 Key usage.....	9
4.3.3 Certificate policies.....	10
4.3.4 Policy mappings.....	10
4.3.5 Subject alternative name	10
4.3.6 Issuer alternative name	10
4.3.7 Subject directory attributes	11
4.3.8 Name constraints	11
4.3.9 Policy constraints.....	11
4.3.10 Extended key usage	11
4.3.11 CRL distribution points	11
4.3.12 Inhibit any-policy.....	11
4.4 IETF RFC 5280 internet certificate extensions	11
4.4.1 Authority Information Access.....	11
5 EU Qualified Certificate requirements.....	12
5.1 EU QCStatements.....	12
5.2 Certificate policies.....	12
History	13

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 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].

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

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.

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 V2.1.1:2016](https://standards.iteh.ai/catalog/standards/sist/128c809d-7baf-4137-903f-7acae06d3311/sist-en-319-412-2-v2-1-1-2016)

<https://standards.iteh.ai/catalog/standards/sist/128c809d-7baf-4137-903f-7acae06d3311/sist-en-319-412-2-v2-1-1-2016>

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 primarily 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

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] 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 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.

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 Definitions and abbreviations

3.1 Definitions

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

3.2 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.

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).