Draft ETSI EN 319 412-3 V1.1.3 (2020-04)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

Reference

REN/ESI-0019412-3v121

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

Important notice

Copyright Notification

Contents

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

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.2] which are used for the security of communications and data for a wide range of electronic applications.

Regulation (EU) No 910/2014 [i.3] 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.1] 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 and interoperable 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.

ETSI EN 319 412-2 [2] specifies a profile for certificates issued to natural persons, which provides the basis for this profile for certificates issued to legal persons.

The present document aims to maximize the interoperability of systems issuing and using certificates both in the European context under the Regulation (EU) No 910/2014 [i.3] and in the wider international environment.

1 Scope

The present document specifies a certificate profile for certificates issued to legal persons. The profile defined in the present document builds on requirements defined in ETSI EN 319 412-2 [2].

The present document supports the requirements of EU qualified certificates as specified in the Regulation (EU) No 910/2014 [i.3] as well as other forms of certificate.

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

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

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

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

[i.3] 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.4] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 412-2 [2] apply.

4 Profile requirements

4.1 Generic requirements

All certificate fields and extensions shall comply with ETSI EN 319 412-2 [2] with the amendments specified in the present document.

4.2 Basic certificate fields

4.2.1 Subject

Clause 4.2.4 of ETSI EN 319 412-2 [2] shall not apply.

The subject field shall include at least the following attributes as specified in Recommendation ITU-T X.520 [1]:

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

Only one instance of each of these attributes shall be present. Additional attributes may be present.

The `countryName` attribute shall specify the country in which the subject (legal person) is established.

The `organizationName` attribute shall contain the full registered name of the subject (legal person).

The `organizationIdentifier` attribute shall contain an identification of the subject organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5 of ETSI EN 319 412-1 [i.4].

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

If present, the size of `organizationName`, `organizationalUnitName` and `commonName` may be longer than the limit as stated in IETF RFC 5280 [3].

NOTE: If other limits are applied it is expected that this is stated in the TSP's published certification practice statement or terms and conditions.

4.3 Standard certificate extensions

4.3.1 Key usage

Clause 4.3.2 of ETSI EN 319 412-2 [2] shall not apply, except those parts which are referenced below.

Clause 4.3.2 of ETSI EN 319 412-2 [2] paragraph 1 and subsequent table 1 shall apply.

Certificates used to validate digital signatures over content (e.g. documents, agreements and/or transactions) that provide evidence of origin and integrity of the content shall be limited to type A, B or F. Of these alternatives, type A should be used (see the security note 2 below).

EXAMPLE: Digital signatures which are aimed to be used as advanced electronic seals as defined in Regulation (EU) No 910/2014 [i.3] are considered to provide evidence of origin and integrity of the content.

NOTE 1: See note 1 in clause 4.3.2 of ETSI EN 319 412-2 [2].

NOTE 2: See note 2 in clause 4.3.2 of ETSI EN 319 412-2 [2].

Annex A (informative):
Change History

Date	Version	Information about changes
February 2020	1.1.2	Implemented Change Requests: • on key usage as in ESI(18)63_051r1 • on IETF RFC 5280 size limits not applying to naming attributes as in ESI(19)000170r2
April 2020	1.1.3	ESI(20)000025: Change Request to Clarify keyUsage in certificates for e-seals ESI(20)000026: Change Request to enhance unrestricted size fields in Subject Version approved by TC ESI for submission to EN Approval Procedure On https://docbox.etsi.org/esi/Open/Compared_deliverables, one will be able to see what changes have taken place between the previous published version (v1.1.1) and this version

History

Document history		
V1.0.1	July 2015	Publication as ETSI TS 119 412-3 (withdrawn)
V1.1.1	February 2016	Publication
V1.1.3	April 2020	EN Approval Procedure AP 20200705: 2020-04-06 to 2020-07-06