# Draft ETSI EN 319 412-2 V2.0.15 (2015-06)


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

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

# Contents

# 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 (http://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 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.

| **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): | 12 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 ITU 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 electronic 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.

# 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

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] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[4] IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".

[5] IETF RFC 2255: "The LDAP URL Format".

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

[7] 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 EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements".

# 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 |
| RSA | Algorithm invented by Rivest, Adleman and Shamir |
| SHA | Secure Hash Algorithm |
| URI | Uniform Resource Identifier |

# 4 Void

# 5 General certificate profile requirements

## 5.1 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].

## 5.2 Basic certificate fields

### 5.2.1 Version

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

### 5.2.2 Void

### 5.2.3 Signature

Signature algorithm shall be selected according to ETSI TS 119 312 [3].

### 5.2.4 Issuer

#### 5.2.4.1 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 [7]:

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

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. 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 need not be an exact match of the fully registered organization name.

NOTE: Earlier editions of X.520 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 X.520. Interoperability issues can arise due to current implementations of X.520 still operating in accordance with the previous size limitations.

#### 5.2.4.2 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 [7]:

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

Additional attributes may be present.

The `countryName` attribute shall specify a country that is consistent with the legal jurisdiction under which certificates are issued.

Other attributes listed above shall comply with requirements stated in clause 5.2.6.

### 5.2.5 Void

### 5.2.6 Subject

The subject field shall include the following attributes as specified in Recommendation ITU-T X.520 [7]:

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

If these mandatory attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the `serialNumber` shall be present.

The subject field shall not contain more than one instance of `commonName` and `countryName`. The `pseudonym` attribute shall not be present if the `givenName` and `surname` attribute are present. Additional attributes other than those listed above may be present. In particular, when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as `organizationName` and `organizationIdentifier`. Certificates may include one or more semantics identifiers as specified in ETSI EN 319 412-1 [i.4], clause 5 which defines the semantics for the `organizationIdentifier` attribute.

The `countryName` attribute value specifies a general context in which other attributes are to be understood. The verifier may have to consult the certificate policy of the issuer to determine the exact semantics of this attribute.

The `serialNumber` attribute has no defined semantics beyond ensuring uniqueness of subject names. It may contain a number or code assigned by the CA or an identifier assigned by a government or civil authority. It is the CA's responsibility to ensure that the `serialNumber` is sufficient to resolve any subject name collisions. Certificates may include one or more semantics identifiers as specified in ETSI EN 319 412-1 [i.4], clause 5 which define the semantics for the `serialNumber` attribute.

The `commonName` attribute value shall contain a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used.

NOTE: The `commonName` attribute has a usage purpose that is different from the required choice of `pseudonym` or `givenName`/`surname`. `commonName` is used for user friendly representation of the person's name, whereas `givenName`/`surname` is used where more formal representation or verification of specific identity of the user is required. To maximize interoperability both are considered necessary.

### 5.2.7 Subject public key info

The subject public key shall be selected according to ETSI TS 119 312 [3].

# 5.3 Void

# 5.4 Standard certificate extensions

## 5.4.1 Authority key identifier

The authority key identifier extension shall be present, containing a key identifier for the issuing CA's public key.

## 5.4.2 Void

## 5.4.3 Key usage

Certificates shall include one (and only one) of the key usage settings defined in table 1 (A, B, C, D, E or F).

**Table 1: Key usage settings**

| Type | Non-Repudiation (Bit 1) | Digital Signature (Bit 0) | Key Encipherment or Key Agreement (Bit 2 or 4) |
|---|---|---|---|
| A | X | | |
| B | X | X | |
| C | | X | |
| D | | X | X |
| E | | | X |
| F | X | X | X |

Certificates used to validate commitment to signed content, such as electronic signatures on agreements and/or transactions, shall be limited to type A, B or F. Of these alternatives, type A should be used (see the security note 3 below).

If the certificate is a qualified certificate then the key usage setting shall be limited to type A, B, C, D or F.

NOTE 1: The X.509 standard [i.3] has renamed the nonRepudiation bit to "contentCommitment". IETF RFC 5280 [1] has kept the original name nonRepudiation for backwards compatibility reasons. These bits are equivalent in function and meaning regardless of their different names.

NOTE 2: **[security note]** Combining the non-repudiation bit (bit 1) in the keyUsage certificate extension with other keyUsage bits can have security implications depending on the security environment in which the certificate is to be used.

If the subject's environment can be fully controlled and trusted, then there are no specific security implications. For example, in cases where the subject is fully confident about exactly which data is signed or cases where the subject is fully confident about the security characteristics of the authentication protocol being used.

If the subject's environment is not fully controlled or not fully trusted, then unintentional signing of commitments is possible. Examples include the use of badly formed authentication exchanges and the use of a rogue software component.

If untrusted environments are used by a subject, these security implications can be limited through use of the following measures:

- to not combine non-repudiation key usage setting in certificates with any other key usage setting and to use the corresponding private key only with this certificate;
- to limit the use of private keys associated with certificates that have the non-repudiation key usage bit set, to environments which are considered adequately controlled and trustworthy.

### 5.4.4 Void

### 5.4.5 Certificate policies

This extension should not be marked critical.

The certificate policies extension shall contain the identifier of at least one certificate policy which reflects the practices and procedures undertaken by the CA.

### 5.4.6 Policy mappings

This extension shall not be present. This extension is not applicable to end entity certificates addressed by the present document.

### 5.4.7 Subject alternative name

This extension shall not be marked critical.

### 5.4.8 Issuer alternative name

This extension shall not be marked critical.

### 5.4.9 Subject directory attributes

The subject directory attributes extension, if present, shall not be used to store any of the identification attribute listed in clause 5.2.6.

### 5.4.10 Void

### 5.4.11 Name constraints

This extension shall not be present. This extension is not applicable to end entity certificates addressed by the present document.

### 5.4.12 Policy constraints

This extension shall not be present. This extension is not applicable to end entity certificates addressed by the present document.

### 5.4.13 Extended key usage

This extension shall not be marked critical.

### 5.4.14 CRL distribution points

The CRL distribution point extension may be present in certificates that include a reference to OCSP in accordance with clause 5.5.1.

If the certificate does not include any reference to OCSP, then the certificate shall include a CRL distribution point extension.

The CRL distribution point extension shall include at least one reference to a publicly available CRL.

At least one of the present references shall use either http (http://) IETF RFC 2616 [4] or ldap (ldap://) IETF RFC 2255 [5] scheme.

The extension shall not be marked critical.

### 5.4.15 Inhibit any-policy

This extension shall not be present. This extension is not applicable to end entity certificates addressed by the present document.

### 5.4.16 Void

## 5.5 IETF RFC 5280 internet certificate extensions

### 5.5.1 Authority Information Access

The Authority Information Access extension shall be present.

When the issuing CA is not represented by a self-signed root certificate, the Authority Information Access extension shall include an `accessMethod` OID, `id-ad-caIssuers`, with an `accessLocation` value specifying at least one access location of a valid CA certificate of the issuing CA. At least one access location should use the http (http://) IETF RFC 2616 [4] scheme. This requirement may be ignored altogether when the issuing CA is represented by a self signed root certificate.

The Authority Information Access extension may include an `accessMethod` OID, `id-ad-ocsp`, with an `accessLocation` value specifying at least one access location of an OCSP [i.2] responder authoritative to provide certificate status information for the present certificate. At least one access location shall specify either the http (http://) IETF RFC 2616 [4] or https (https://) IETF RFC 2818 [6] scheme. Such access location shall reference a publicly available OCSP responder, which accepts unsigned and unauthenticated status requests.

A reference to at least one OCSP responder shall be present if the certificate does not include any CRL distribution point extension in accordance with clause 5.4.14.

NOTE: An applicable certificate policy can define further requirements on support of revocation services such as CRL and OCSP. For example, see ETSI EN 319 411-1 [i.7].

### 5.5.2 Void

## 5.6 Void

### 5.6.1 Void

### 5.6.2 Void

# 6 EU qualified certificate requirements

## 6.1 EU QCStatements

EU qualified certificates shall include `QCStatements` in accordance with ETSI EN 319 412-5 [2].

## 6.2 Certificate policies

EU qualified certificates should include, in the certificate policies extension, one of the certificate policy identifiers defined in clause 5.2 of ETSI EN 319 411-2 [i.6]. Policy identifiers included in the certificate policies extension of EU qualified certificates shall be consistent with the `QCStatements` according to clause 6.1.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | March 2004 | Publication as ETSI TS 102 280 |
| V1.1.1 | April 2012 | Publication as ETSI TS 119 412-2 |
| V1.2.1 | August 2013 | Publication as ETSI TS 119 412-2 |
| V2.0.15 | June 2015 | EN Approval Procedure AP 20151016: 2015-06-18 to 2015-10-16 |
| | | |