Draft ETSI EN 319 412-2 V2.3.0 (2023-06)

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

Reference
REN/ESI-0019412-2v231

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

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 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 Certificate 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].

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.

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 certificate 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.

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 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] 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.

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".

[i.9] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

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 following abbreviations apply:

CA	Certification Authority
CRL	Certificate Revocation List
DN	Distinguished name
EC	European Commission
EU	European Union
ISO	International Standards Organization
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
RFC	Request For Comments
TSP	Trust Service Provider

3.4 Notations

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

4 General certificate profile requirements

4.1 Generic requirements

GEN-4.1-1: All certificate fields and extensions shall comply with IETF RFC 5280 [1] with the amendments specified in the present document.

GEN-4.1-2: 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

GEN-4.2.1-1: The version shall be V3 (defined by the integer value 2).

4.2.2 Signature

GEN-4.2.2-1: 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

GEN-4.2.3.1-1: If the issuer is a legal person the following requirements shall apply:

GEN-4.2.3.1-2: The identity of the issuer, shall contain at least the following attributes as specified in Recommendation ITU-T X.520 [6]:

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

GEN-4.2.3.1-3: If an appropriate registration number is known to exist, then the identity of the issuer shall contain organizationIdentifier and with value different from the organization name.

EXAMPLE: An appropriate registration number can be listed in a ETSI TS 119 612 [i.9] trusted list.

GEN-4.2.3.1-4: Certificates may include a legal person semantic identifier as specified in clause 5.1.4 of ETSI EN 319 412-1 [i.4].

GEN-4.2.3.1-5: Each attribute shall be limited to a single instance of the attribute. Additional attributes may be present.

GEN-4.2.3.1-6: The `countryName` attribute shall specify the country in which the issuer of the certificate is established.

GEN-4.2.3.1-7: The `organizationName` attribute shall contain the full registered name of the certificate issuing organization.

GEN-4.2.3.1-8: The `organizationIdentifier` attribute shall contain an identification of the certificate issuing organization different from the organization name.

GEN-4.2.3.1-9: 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

GEN-4.2.3.2-1: If the issuer is a natural person the following requirements shall apply:

GEN-4.2.3.2-2: The identity of the issuer shall contain at least the following attributes as specified in Recommendation ITU-T X.520 [6]:

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

GEN-4.2.3.2-3: Each attribute shall be limited to a single instance of the attribute. Additional attributes may be present.

GEN-4.2.3.2-4: The countryName attribute shall specify a country that is consistent with the legal jurisdiction under which certificates are issued.

GEN-4.2.3.2-5: In case of the (givenName and/or surname) alternative, if the given name of the issuer is known, then the givenName attribute shall be present.

GEN-4.2.3.2-6: In case of the (givenName and/or surname) alternative, if the surname of the issuer is known, then the surname attribute shall be present.

NOTE 1: Some natural persons do not have both a given name and a surname.

NOTE 2: Regulation (EU) No 910/2014 [i.5] does not allow the usage of pseudonym for natural person issuers.

GEN-4.2.3.2-7: Other attributes listed above shall comply with requirements stated in clause 4.2.4.

NOTE 3: 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.

4.2.4 Subject

NAT-4.2.4-1: The subject field shall include the following attributes as specified in Recommendation ITU-T X.520 [6]:

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

NAT-4.2.4-2: If these mandatory attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber shall be present.

NAT-4.2.4-3: The subject field shall not contain more than one instance of commonName and countryName.

NAT-4.2.4-4: The `pseudonym` attribute shall not be present if the `givenName` and `surname` attribute are present.

NAT-4.2.4-5: Additional attributes other than those listed above may be present.

NAT-4.2.4-6: 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`.

NAT-4.2.4-7: 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.

NAT-4.2.4-8: 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.

NAT-4.2.4-9: 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.

NAT-4.2.4-10: In case of the (`givenName` and/or `surname`) alternative, if the given name of the subject is known, then the `givenName` attribute shall be present.

NAT-4.2.4-11: In case of the (`givenName` and/or `surname`) alternative, if the surname of the subject is known, then the `surname` attribute shall be present.

NOTE 1: Some natural persons do not have both a given name and a surname.

NAT-4.2.4-12: The givenName with surname shall contain formal representation of the user's identity, such as indicated on a user's official identity document.

NAT-4.2.4-13: The CA shall ensure that the `serialNumber` is sufficient to resolve any subject name collisions.

NAT-4.2.4-14: 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.

NAT-4.2.4-15: The `commonName` attribute value shall contain a name of the subject.

NAT-4.2.4-16: The `commonName` attribute value may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format.

NAT-4.2.4-17: Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used in the `commonName` attribute value.

NOTE 2: 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.

NAT-4.2.4-18: If present, the size of `givenName`, `surname`, `pseudonym`, `commonName`, `organizationName` and `organizationalUnitName` may be longer than the limit as stated in IETF RFC 5280 [1].

NOTE 3: If other limits are applied it is expected that this is stated in the TSP's published certification practice statement or terms and conditions.

NAT-4.2.4-19: The CA should not use different language encoding between subject DN fields "givenName", "surname" and "commonName".

EXAMPLE: "C=GR, givenName=Δημήτριος, surname=Ζαχαρόπουλος, commonName=Dimitrios Zacharopoulos" is not allowed.

NAT-4.2.4-20: If the CA wants to include the Subject's name in the certificate with an additional encoding national or latin, it may use the Subject Alternative Name extension for this purpose and add the values using the directoryName value type.