ETSI EN 319 412-2 V2.4.1 (2025-06)

EUROPEAN STANDARD

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

Reference

REN/ESI-0019412-2v241

Keywords

electronic signature, IP, profile, security, trust services

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

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 on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to
the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

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].

National transposition dates	
Date of adoption of this EN:	12 June 2025
Date of latest announcement of this EN (doa):	30 September 2025
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 March 2026
Date of withdrawal of any conflicting National Standard (dow):	31 March 2026

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 in the ETSI docbox.

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 Trust 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".

[7] ICAO Doc 9303: "Machine Readable Travel Documents; Part 3: Specifications Common to all MRTDs".

[8] IETF RFC 9608: "No Revocation Available for X.509 Public Key Certificates".

## 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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[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 Trust 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 (eIDAS).

[i.6]	ETSI EN 319 411-2: "Electronic Signatures and Trust 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 Trust 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 Trust Infrastructures (ESI); Trusted Lists".

[i.10]	ETSI EN 319 411-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

# 3	Definition of terms, symbols, abbreviations and notations

## 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/or 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-4.2.4-12A: (CONDITIONAL) If the givenName and/or Surname formal representation needs transliteration then that transliteration shall follow the actual edition of ICAO Doc 9303 Part 3 [7] Section 6. A. *Transliteration of Multinational Latin-Based Characters*.

> NOTE 2:   The fact and reason for the transliteration are to be recorded as part of the registration and lifecycle information in the audit log in accordance with ETSI EN 319 411-1 [i.10], clause 6.4.5.

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 3:   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 4:   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.

4.2.5   Subject public key info

GEN-4.2.5-1: The subject public key 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.

4.3   Standard certificate extensions

4.3.1   Authority key identifier

GEN-4.3.1-1: The authority key identifier extension shall be present, containing a key identifier for the issuing CA's public key.

4.3.2   Key usage

NAT-4.3.2-1: The key usage extension shall be present and shall contain one (and only one) of the key usage settings defined in table 1 (A, B, C, D, E or F). Type A, C or E should be used to avoid mixed usage of keys.

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

NAT-4.3.2-2: Certificates used to validate commitment to signed content (e.g. documents, agreements and/or transactions) shall be limited to type A, B or F.

NAT-4.3.2-3: 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 signatures as defined in Regulation (EU) No 910/2014 [i.5] are considered to signal commitment to signed content.

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.

4.3.3 Certificate policies

GEN-4.3.3-1: This extension should not be marked critical.

GEN-4.3.3-2: The certificate policies extension shall be present and shall contain the identifier of at least one certificate policy which reflects the practices and procedures undertaken by the CA.

4.3.4 Policy mappings

GEN-4.3.4-1: This extension shall not be present. This extension is not applicable to end entity certificates addressed by the present document.

4.3.5 Subject alternative name

GEN-4.3.5-1: This extension shall not be marked critical.

4.3.6 Issuer alternative name

GEN-4.3.6-1: This extension shall not be marked critical.

4.3.7 Subject directory attributes

GEN-4.3.7-1: The subject directory attributes extension, if present, shall not be used to store any of the identification attribute listed in clause 4.2.5.

4.3.8 Name constraints

GEN-4.3.8-1: This extension shall not be present. This extension is not applicable to end entity certificates addressed by the present document.

4.3.9 Policy constraints

GEN-4.3.9-1: This extension shall not be present. This extension is not applicable to end entity certificates addressed by the present document.

4.3.10   Extended key usage

GEN-4.3.10-1: This extension shall not be marked critical.

4.3.11   CRL distribution points

GEN-4.3.11-1: If CRL is supported by the issuing CA, the CRL distribution point extension shall be present in certificates.

GEN-4.3.11-1A: For OCSP responder certificates the requirements in the present clause shall not apply.

GEN-4.3.11-2: If the certificate does not include any access location of an OCSP responder as specified in clause 4.4.1, and the certificate does not include the validity assured extension as defined in ETSI EN 319 412-1 [i.4], then the certificate shall include a CRL distribution point extension.

GEN-4.3.11-2A: If a certificate includes the validity assured extension, but neither include a CRL distribution point nor access location of an OCSP responder (as specified in clause 4.4.1) is included, then the certificate shall have No Revocation Available extensions as specified in IETF RFC 9608 [8].

> NOTE: A validity assured certificate does not need to have CRL distribution point extension or access location of an OCSP responder (as specified in clause 4.4.1) included in the certificate, but it is allowed for compatibility reasons to have those. (Because most of the software available at the moment needs revocation info.) If none of them included, then the No Revocation Available extension is mandatory to fulfil the eIDAS [i.5], Annex I (i).

GEN-4.3.11-3: When present, the CRL distribution point extension shall include at least one reference to a publicly available CRL.

GEN-4.3.11-4: At least one of the present references shall use either http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme.

GEN-4.3.11-5: The extension shall not be marked critical.

4.3.12   Inhibit any-policy

GEN-4.3.12-1: This extension shall not be present. This extension is not applicable to end entity certificates addressed by the present document.

4.4   IETF RFC 5280 internet certificate extensions

4.4.1   Authority Information Access

GEN-4.4.1-1: For OCSP responder certificates the requirements in the present clause shall not apply.

GEN-4.4.1-2: The Authority Information Access extension shall be present.

GEN-4.4.1-3: 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.

GEN-4.4.1-4: At least one `accessLocation` shall use the http (http://) IETF RFC 7230-7235 [3] scheme or https (https://) IETF RFC 2818 [5] scheme.

GEN-4.4.1-5: If OCSP is supported by the issuing CA, the Authority Information Access extension shall 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.

GEN-4.4.1-6: If OCSP is supported by the issuing CA, at least one access location shall specify either the http (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5] scheme.

GEN-4.4.1-7: If OCSP is supported by the issuing CA, the access location shall reference a publicly available OCSP responder, which accepts unsigned and unauthenticated status requests.

GEN-4.4.1-8: If the certificate does not include any CRL distribution point extension in accordance with clause 4.3.11, and the certificate does not include the validity assured extension as defined in ETSI EN 319 412-1 [i.4], a reference to at least one OCSP responder shall be present.

GEN-4.4.1-8A: If a certificate includes the validity assured extension, but neither include a CRL distribution point nor access location of an OCSP responder (as specified in clause 4.4.1) is included, then the certificate shall have No Revocation Available extensions as specified in IETF RFC 9608 [8].

> NOTE: A validity assured certificate does not need to have CRL distribution point extension or access location of an OCSP responder (as specified in clause 4.4.1) included in the certificate, but it is allowed for compatibility reasons to have those. (Because most of the software available at the moment needs revocation info.) If none of them included, then the No Revocation Available extension is mandatory to fulfil the eIDAS [i.5], Annex I (i).

5   EU Qualified Certificate requirements

5.1   EU QCStatements

QCS-5.1-1: If certificates are issued as EU Qualified Certificates, they shall include QCStatements in accordance with ETSI EN 319 412-5 [2].

5.2   Certificate policies

QCS-5.2-1: When certificates are issued as EU Qualified Certificates, they should include, in the certificate policies extension, one of the certificate policy identifiers defined in clause 5.3 of ETSI EN 319 411-2 [i.6].

QCS-5.2-2: Policy identifiers included in the certificate policies extension of EU Qualified Certificates shall be consistent with the QCStatements according to clause 5.1.

Annex A (informative):
Change history

Date	Version	Information about changes
February 2020	2.1.2	Implemented Change Requests: • on key usage in ESI(18)63_039r1. • on IETF RFC 5280 size limits not applying to naming attributes in ESI(19)000163r3. • on Authority Information Access in ESI(19)65_011.
April 2020	2.1.3	ESI(20)000024: Change Request to enhance unrestricted Organization Name and Common Name. 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 (v2.1.1) and this version.
April 2023	2.2.6	Updated to allocate reference number to each requirement in line with ETSI EN 319 411-1. CR#1 Withdrawn. CR#2 Specifying where to include the local language. CR#3 handle the case of natural persons without a given name (or surname). CR#4 Remove pseudonym for natural person issuer. CR#5 Replace "should" by "shall" in the new text clarifying given name and surname. CR#6 Adapt history. CR#7 No contribution. CR#8 Inclusion of OrganizationIdentifier for issuer.
February 2025	2.3.2	Addition of NoRevAvail extension, in the case when neither OCSP accespoint, nor CDP included in the certificate and other relevant corrections (CR#1). Correction of NAT-4.2.4-4 (CR#2). Addition of transliteration rules to NAT-4.2.4-12A (CR#3). Addition of an exception to clause 4.3.11 as 4.3.11-1A (CR#4).

History

Document history			
V1.1.1	March 2004	Publication as ETSI TS 102 280 (Historical)	
V1.1.1	April 2012	Publication as ETSI TS 119 412-2 (Withdrawn)	
V1.2.1	August 2013	Publication as ETSI TS 119 412-2 (Withdrawn)	
V2.0.16	July 2015	Publication as ETSI TS 119 412-2 (Withdrawn)	
V2.1.1	February 2016	Publication	
V2.2.1	July 2020	Publication	
V2.3.1	September 2023	Publication	
V2.4.0	March 2025	ENAP process	AP 20250612: 2025-03-14 to 2025-06-12
V2.4.1	June 2025	Publication	