Draft ETSI EN 319 412-1 V1.4.2 (2020-07)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

Reference

REN/ESI-0019412-1v142

Keywords

e-commerce, electronic signature, 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

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

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 1 of a multi-part deliverable covering the Certificate Profiles, as identified below:

Part 1: "Overview and common data structures";

Part 2: "Certificate profile for certificates issued to natural persons";

Part 3: "Certificate profile for certificates issued to legal persons";

Part 4: "Certificate profile for web site certificates";

Part 5: "QCStatements".

The present document was previously published as ETSI TS 119 412-1 [i.14].

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 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.9] 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], superseded by the Regulation (EU) No 910/2014 [i.9], 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 certificate 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.9] and in the wider international environment.

1 Scope

The present document provides an overview of the Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3] based certificate profiles and the statements for EU Qualified Certificates specified in other parts of ETSI EN 319 412 ([i.4] to [i.7]). It specifies common data structures that are referenced from other parts of ETSI EN 319 412 ([i.4] to [i.7]).

The profiles specified in this multi-part deliverable aim to support both the Regulation (EU) No 910/2014 [i.9] and use of certificates in a wider international context. Within the European context, it aims to support both EU Qualified Certificates and 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] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[2] ISO 3166: "Codes for the representation of names of countries and their subdivisions".

[3] ETSI TS 119 495: "Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366".

[4] ISO 17442: "Financial services -- Legal Entity Identifier (LEI)".

[5] eIDAS: "SAML Attribute Profile v1.2", 31 August 2019.

NOTE: Available at https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf?version=2&modificationDate=1571068651772&api=v2.

[6] IETF RFC 5912: "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)".

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] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

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

[i.5] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for certificates issued to legal persons".

[i.6] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate Profile for web site certificates".

[i.7] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[i.8] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.9] 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.10] Recommendation ITU-T X.520 (10/2012): "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[i.11] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.12] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax.

[i.13] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[i.14] ETSI TS 119 412-1: "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 319 401 [i.2] and the following apply:

EU Qualified Certificate: qualified certificate that is stated to be in accordance with annex I, III or IV of the Regulation (EU) No 910/2014 [i.9] or annex I of the Directive 1999/93/EC [i.1] whichever is in force at the time of issuance

short-term certificate: certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in the certificate practice statement

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
OID	Object IDentifier
LEI	Legal Entity Identifier
SAML	Security Assertion Markup Language
TLS	Transport Layer Security protocol

NOTE: As specified in IETF RFC 5246 [i.8].

TSP	Trust Service Provider
UN	United Nations

4 ETSI EN 319 412 certificate profiles

4.1 General approach

All the certificate profiles specified in ETSI EN 319 412 are based upon IETF RFC 5280 [i.11] for generic profiling of Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3]. The certificate profiles specify profiles for both EU Qualified Certificates and non-qualified certificates as relevant. Reference is made to ETSI EN 319 412-5 [i.7] for requirements relating to `QCStatements`.

4.2 Overview of other parts of ETSI EN 319 412

4.2.1 ETSI EN 319 412-2

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

Scope: This part specifies the requirements on certificate content for TSPs issuing certificates to natural persons. It provides a certificate profile, which facilitates interoperability of certificates issued to natural persons for the purposes of supporting digital signatures, peer entity authentication, data authentication as well as data confidentiality. It specifies a profile for both EU Qualified Certificates as specified in the Regulation (EU) No 910/2014 [i.9], and non-qualified certificates. When certificates for natural persons are issued as EU Qualified Certificates, it makes reference to ETSI EN 319 412-5 [i.7] for requirements relating to `QCStatements`.

4.2.2 ETSI EN 319 412-3

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

Scope: This part specifies the requirements on certificate content for TSPs issuing certificates to legal persons. It provides a certificate profile, which facilitates interoperability of certificates issued to legal persons for the purposes of supporting digital signatures, peer entity authentication, data authentication as well as data confidentiality. It specifies a profile for both EU Qualified Certificates and non-qualified certificates. When certificates for legal persons are issued as EU Qualified Certificates, it makes reference to ETSI EN 319 412-5 [i.7] for requirements relating to `QCStatements`.

4.2.3 ETSI EN 319 412-4

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.

Scope: This part specifies the requirements on certificate content for TSPs issuing website certificates for sites that are accessed via the TLS protocol as specified in IETF RFC 5246 [i.8]. It provides a certificate profile, which enables interoperability of website certificates issued to legal or natural persons. It specifies a profile for both EU Qualified Certificates and non-qualified certificates. When certificates for web site authentication are issued as EU Qualified Certificates, it makes reference to ETSI EN 319 412-5 [i.7] for requirements relating to `QCStatements`.

4.2.4 ETSI EN 319 412-5

Electronic Signatures and Infrastructures (ESI) ; Certificate Profiles ; Part 5 : QCStatements.

Scope: This part specifies the requirements on the `QCStatements` as required for qualified certificates as specified in parts 2 to 4 [i.4], [i.5] and [i.6] of ETSI EN 319 412.

The `QCStatements` defined in clause 4.3 of ETSI EN 319 412-5 [i.7] may be applied to regulatory environments outside the EU. Other requirements specified in clause 4 are specific to Regulation (EU) No 910/2014 [i.9] but may be adapted for other regulatory environments.

5 Common data structures

5.1 Semantics identifiers

5.1.1 General

Subject and issuer names (Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3]) can include attributes that do not disclose the semantics of its information content. `serialNumber` (Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3]) and `organizationIdentifier` (Recommendation ITU-T X.520 [i.10]) are examples of such attributes. The `serialNumber` attribute can contain a national identification number, passport number or any type of locally defined identifier such as random or pseudo-random generated identifier. The `organizationIdentifier` attribute can contain several types of organizational identifiers.

IETF RFC 3739 [1], clause 3.2.6.1 defines the predefined statement "qcStatement-2" identified by the OID id-qcs-pkixQCSyntax-v2 with the `SemanticsInformation` syntax.

The `SemanticsInformation` type, when present, provides information about the semantics of data stored in attributes and/or names in the certificate.

The semantics identifiers in the following clauses use 2 character ISO 3166 [2] country codes (Alpha-2) to specify the country where the identifier is registered. Trans-national country codes as specified in ISO 3166 [2] may be used when relevant such as EU (European Union) and UN (United Nations). User-defined country code 'XG' may be used for identifiers allocated under a global scheme. Identifiers using user-defined country codes shall be interpreted under the context of the certificate issuer as there is no guarantee that such identifier is unique across all issuers. Unassigned codes should not be used.

NOTE: The semantics identifiers in the following clauses define semantics information for attributes stored in the subject field. No corresponding mechanism is defined in the present document for specifying semantics information for attributes in the issuer field. IETF RFC 5280 [i.11] path validation requires the issuer field to be consistent with the subject field of the CA certificate assigned to the issuing CA. Name attributes of the issuing CA can be constructed according the semantics identifier defined in the following clauses and stored in the subject field of the CA certificate. In such case, the appropriate place to include semantics identifiers for these attributes is in the CA certificate. Consequently, a relying party will have to consult information in the issuing CA certificate to obtain semantics information about attributes in the issuer field of a certificate.