Draft ETSI EN 319 412-1 V1.0.0 (2015-06)

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

Reference
DEN/ESI-0019412-1

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

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 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 issued to organizations";

Part 5: "QCStatements".

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 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 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 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 maximise 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 X.509 | ISO/IEC 9594-8 [i.3] based certificate profiles and the statements for 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 document 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 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 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

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

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 issued to organisations".

[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".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions 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

3.2 Abbreviations

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

ASN.1 Abstract Syntax Notation 1
OID Object Identifier
SSL Secure Socket Layer

NOTE: This is an earlier version of the TLS protocol defined in IETF RFC 5246 [i.8].

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 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 electronic signatures, peer entity authentication, data authentication as well as data confidentiality. It specifies a profile for both qualified as specified in the Regulation (EU) No 910/2014 [i.9], and non-qualified certificates. When certificates for natural persons are issued as 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 electronic signatures and electronic seals (as defined in the Regulation (EU) No 910/2014 [i.9]), peer entity authentication, data authentication as well as data confidentiality. It specifies a profile for both qualified and non-qualified certificates. When certificates for legal persons are issued as 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 issued to organizations.

Scope: This part specifies the requirements on certificate content for TSPs issuing website certificates to organisations for sites accessible via the TLS protocol [i.8] and earlier equivalents such as SSL. It provides a certificate profile, which enables interoperability of website certificates issued to organisations. It specifies a profile for both qualified and non-qualified certificates. When certificates for web site authentication are issued as 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 [i.4] to 4 [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 (X.509 [i.3]) can include attributes that do not disclose the semantics of its information content. `serialNumber` (X.509 [i.3]) and `organizationIdentifier` (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. 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 ISO 3166 [2] country codes 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 codes (AA, QM-QZ, XA-XZ and ZZ) may be used for other trans-national identifiers. 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.

5.1.2 ASN.1 module

This clause defines two semantics identifiers for inclusion in qcStatement-2.

The syntax for the natural person semantics identifier and legal person semantics identifier shall be as defined by the following ASN.1 module:

```
ETSISemanticsIdentifierMod { itu-t(0) identified-organization(4) etsi(0) id-cert-profile(194121)
id-mod(0) id-mod-semantics-identifier(0) }


DEFINITIONS EXPLICIT TAGS::=

BEGIN

-- EXPORTS All --

-- Semantics identifiers

id-etsi-qcs-semantics-identifiers     OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4)
etsi(0) id-cert-profile(194121) 1 }

-- Semantics identifier for natural person identifier

id-etsi-qcs-semanticsId-Natural     OBJECT IDENTIFIER ::= { id-etsi-qcs-semantics-identifiers 1 }

-- Semantics identifier for legal person identifier

id-etsi-qcs-SemanticsId-Legal     OBJECT IDENTIFIER ::= { id-etsi-qcs-semantics-identifiers 2 }

END
```

The following clauses provide the semantics definitions of the natural person and legal person semantics identifiers.

5.1.3 Natural person semantics identifier

The semantics of `id-etsi-qcs-SemanticsId-Natural` shall be as follows.

When the natural person semantics identifier is included, any present `serialNumber` attribute in the subject field shall contain information using the following structure in the presented order:

- 3 character natural identity type reference;
- 2 character ISO 3166 [2] country code;
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- identifier (according to country and identity type reference).

The three initial characters shall have one of the following defined values:

1) "PAS" for identification based on passport number.
2) "IDC" for identification based on national identity card number.
3) "PNO" for identification based on (national) personal number (national civic registration number).
4) "TAX" for identification based on a personal tax reference number issued by a national tax authority. This value is **deprecated.** The value "TIN" should be used instead.
5) "TIN" Tax Identification Number according to the European Commission – Tax and Customs Union (https://ec.europa.eu/taxation_customs/tin/tinByCountry.html). Or
6) Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).

Other initial character sequences are reserved for future amendments of the present document.

EXAMPLES: "PASSK-P3000180", "IDCBE-590082394654" and "EI:SE-200007292386".

When a locally defined identity type reference is provided (two characters followed by ":"), the `nameRegistrationAuthorities` element of `SemanticsInformation` (IETF RFC 3739 [1]) shall be present and shall contain at least a `uniformResourceIdentifier` `generalName`. The two letter identity type reference preceding the ":" character shall be unique within the context of the specified `uniformResourceIdentifier`.

5.1.4 Legal person semantics identifier

The semantics of `id-etsi-qcs-SemanticsId-Legal` shall be as follows.

When the legal person semantics identifier is included, any present `organizationIdentifier` attribute in the subject field shall contain information using the following structure in the presented order:

- 3 character legal person identity type reference;
- 2 character ISO 3166 [2] country code;
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- identifier (according to country and identity type reference).

The three initial characters shall have one of the following defined values:

1) "VAT" for identification based on a national value added tax identification number.
2) "NTR" for identification based on an identifier from a national trade register. Or

3) Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).

Other initial character sequences are reserved for future amendments of the present document.

EXAMPLES: "VATBE-0876866142" and "EI:SE-5567971433".

When a locally defined identity type reference is provided (two characters followed by ":"), the `nameRegistrationAuthorities` element of `SemanticsInformation` (IETF RFC 3739 [1]) shall be present and shall contain at least a `uniformResourceIdentifier` `generalName`. The two letter identity type reference following the ":" character shall be unique within the context of the specified `uniformResourceIdentifier`.

History

Document history			
V1.0.0	June 2015	EN Approval Procedure	AP 20151016: 2015-06-18 to 2015-10-16