ETSI TS 119 412-2 V1.2.1 (2013-08)

Technical Specification

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

Reference

RTS/ESI-0019412-2

Keywords

electronic signature, IP, profile, security

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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 Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.1].

The present document was previously published as TS 102 280.

Introduction

The present document defines a common profile for X.509 based certificates issued to natural persons.

The Directive of the European Parliament and of the Council on a Community framework for electronic signatures (1999/93/EC [1]) defines requirements on a specific type of certificates named "Qualified Certificates". Implementation of the Directive 1999/93/EC [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.

1 Scope

The present document defines a common profile for Recommendation ITU-T X.509 [2] based certificates issued to natural persons. The scope of the present document is to provide a certificate profile, which will allow actual interoperability of certificates issued for the purposes of qualified electronic signatures, peer entity authentication and data authentication.

This profile depends on the Internet standards RFC 5280 [3] and RFC 3739 [4] for generic profiling of Recommendation ITU-T X.509 [2], and depends on the ETSI standard TS 101 862 [5] to define implementation of requirements defined by the Electronic Signature Directive 1999/93/EC [1] Annexes I and II.

The scope of the present document is primary limited to facilitate interoperable processing and display of certificate information in existing deployments of Recommendation ITU-T X.509 [2]. It is thus important to note that this profile deliberately has excluded support for some certificate information content options, which may 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. Guidance for implementers is provided for cases in which near term developments are affected.

This certificate profile recognizes the natural need for reasonable variations of implementation which does not negatively affect generic interoperability. This is e.g. valid for different ways to encode a certificate holder's identity.

Certain applications or protocols impose specific requirements on certificate content such as IP-sec, Network logon, S/MIME, IEEE 802.1x [12] EAP. 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

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 reference 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.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[2] Recommendation ITU-T X.509/ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

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

[4] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[5] ETSI TS 101 862: "Qualified Certificate profile".

NOTE: This reference will be replaced by EN 319 412-5 [i.2] once it is published.

[6] IETF RFC 2119: "Key words for use in RFCs to Indicate Requirement Levels".

[7] IETF RFC 3279: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[8] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

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

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

[11] IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[12] IEEE 802.1x: "IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control".

[13] IETF RFC 4055: "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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

[15] ISO 3166 (all parts): "Codes for the representation of names of countries and their subdivisions".

2.2 Informative references

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] ETSI TS 119 412-1: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 1: Overview".

[i.2] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile".

3 Abbreviations

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

ASN.1	Abstract Syntax Notation one
CA	Certification Authority
CRL	Certificate Revocation List
DIT	Directory Information Tree
DS	Digital Signature
EAP	Extensible Authentication Protocol
EC	European Commission
KEA	Key Encipherment or Agreement
NR	Non-Repudiation
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
RSA	Rivest, Shamir and Adleman algorithm
SHA	Secure Hash Algorithm

4 Document structure and terminology

4.1 Document structure

The present document profiles the use of other standards.

Clause 4 contains the profiling requirements defined by the present document. This clause does not repeat the base requirements of the referenced standards.

Annex A is an informative annex which, for convenience purposes only, lists some important requirements from referenced standards that are relevant for the understanding of the present document.

4.2 Terminology

The key words "SHALL", "SHALL NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in the present document are to be interpreted as described in RFC 2119 [6].

5 Profile requirements

5.1 Generic requirements

All certificate fields and extensions SHALL, where applicable, comply with RFC 5280 [3], RFC 3739 [4] and TS 101 862 [5] with the amendments specified in the present document. When "No specific requirements" is stated for a particular field or extension, this means that no specific requirements apply except for those stated by RFC 5280 [3], RFC 3739 [4] and TS 101 862 [5]. Certificates declared as Qualified Certificates SHALL fully comply with TS 101 862 [5].

In case of discrepancies between the present specification and the named standards above, the present document is the normative one.

5.2 Basic certificate fields

5.2.1 Version

Certificates compliant with the present document SHALL be Recommendation ITU-T X.509 [2] version 3 certificates.

5.2.2 Serial number

No specific requirements.

5.2.3 Signature

Signature algorithm SHALL be specified according to RFC 3279 [7] and selected according to TS 102 176-1 [8], including any updates and amendments to these standards, or according to applicable national regulation.

5.2.4 Issuer

The identity of the issuer SHALL be specified using an appropriate subset of the following attributes:

```
countryName,
organizationName,
organizationalUnitName, (multiple instances may be present)
stateOrProvinceName,
localityName,
commonName, and
```

```
serialNumber
```

Additional attributes MAY be present but they SHOULD NOT be necessary to identify the issuing organization.

The attributes `countryName` and `organizationName` SHALL be present. The `organizationName` attribute SHALL contain the full registered name of the certificate issuing organization and `countryName` SHALL specify the country in which the issuer of the certificate is established.

5.2.5 Validity

No specific requirements.

5.2.6 Subject

The subject field SHALL contain an appropriate subset of the following attributes:

```
countryName,
commonName,
surname,
givenName,
pseudonym,
serialNumber,
title,
organizationName,
organizationalUnitName,
stateOrProvinceName, and
localityName.
```

Other attributes may be present but SHALL NOT be necessary to distinguish the subject name from other subject names within the issuer domain.

The subject field SHALL include at least one of the following choices of attributes as defined in RFC 3739 [4]:

Choice I: `commonName`

Choice II: `givenName`

Choice III: `pseudonym`

5.2.7 Subject public key info

The subject public key SHALL be specified according to RFC 3279 [7] and selected according to TS 102 176-1 [8], including any updates and amendments to these standards, or according to applicable national regulation.

5.3 X.509 version 2 certificate fields

The Recommendation ITU-T X.509 [2] version 2 certificate fields Issuer and Subject Unique Identifier SHALL NOT be present.

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 Subject key identifier

No specific requirements.

5.4.3 Key usage

The following key usage settings are named in this profile as type A, B, C, D and E:

Type	Non-Repudiation [NR] (Bit 1)	Digital Signature [DS] (Bit 0)	Key Encipherment or Agreement [KEA] (Bit 2 or 4)
A	X		
B	X	X	
C		X	
D		X	X
E			X

Certificates conforming to this profile SHALL include one (and only one) of these key usage settings (A, B, C, D or E).

In cases where a certificate is intended to be used to validate commitment to signed content, such as electronic signatures on agreements and/or transactions, then the key usage combination SHALL be limited to type A or B. This means that the non-repudiation bit (bit 1) SHALL be set. Of these alternatives it is RECOMMENDED to use the type A setting only (see the security note below).

For all other certificates compliant with this profile, key usage settings SHALL be limited to type C, D or E.

If the certificate is declared to be a Qualified Certificate according to TS 101 862 [5] then the key usage setting SHALL be limited to type A, B or C.

NOTE 1: Choice of bit 2 or bit 4 for expressing [KEA] is dependent on the algorithm type specified in subject public key info (clause 5.2.7 Subject public key info). Appropriate values for RSA keys are referenced in clause A.4.3.

NOTE 2: The X.509 standard has renamed the nonRepudiation bit to "contentCommitment". RFC 5280 [3] has kept the original name nonRepudiation for backwards compatibility reasons. These bits are equivalent in function and meaning regardless of their different names.

Security note:

- Combining the non-repudiation bit (bit 1) in the keyUsage certificate extension with other keyUsage bits may 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 Private key usage period

No specific requirements.

5.4.5 Certificate policies

This extension SHOULD NOT be marked critical.

5.4.6 Policy mappings

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 Basic constraints

No specific requirements.

5.4.11 Name constraints

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

5.4.12 Policy constraints

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 SHALL be present.

At least one reference to a publicly available CRL SHALL be present.

At least one of the present references SHALL use either http (http://) RFC 2616 [9] or ldap (ldap://) RFC 2255 [10] scheme.

The extension SHALL NOT be marked critical.

Compliant issuing CAs MAY support other certificate status checking services, such as OCSP, in addition to support of CRL through this extension.

5.4.15 Inhibit any-policy

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

5.4.16 Freshest CRL

No specific requirements.

5.5 RFC 5280 internet certificate extensions

5.5.1 Authority Information Access

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://) RFC 2616 [9] scheme. This requirement MAY be ignored altogether when the issuing CA is represented by a self signed root certificate.

The Authority Information Access extension SHOULD include an `accessMethod` OID, `id-ad-ocsp`, with an `accessLocation` value specifying at least one access location of an OCSP responder authoritative to provide certificate status information for the present certificate. At least one access location SHOULD use either the http (http://) RFC 2616 [9] or https (https://) RFC 2818 [14] scheme. Such access location, when present SHALL reference a publically available OCSP responder, which accepts unsigned and unauthenticated status requests.

5.5.2 Subject information access

No specific requirements.

5.6 RFC 3739 certificate extensions

5.6.1 Biometric information

No specific requirements.

5.6.2 Qualified certificate statement

Certificates declared as Qualified Certificates SHALL comply with TS 101 862 [5] regarding use of this extension.

Certificates issued according to this profile MAY include one or more semantics identifiers, according to annex B, providing relevant semantics definitions to determine the identity of the subject of the certificate.

Annex A (informative): Important requirements from referenced standards

A.1 Scope and structure

Annex A lists important requirements and recommendations from referenced standards which are considered important for implementation of the present document.

Annex A is included for convenience in order to facilitate a better understanding of the requirements of the present document in situations where the reader does not have all referenced standards available or in situations where the reader wishes to obtain a brief understanding of the present document without having to review the complex set of referenced standards. All referenced standards in annex A are listed in clause 2 of the present document.

The list of requirements and recommendations is not exhaustive. The referenced standards are necessary to obtain full understanding of listed requirements and recommendations.

A.2 Basic certificate fields

A.2.1 Version

No specific requirement listed.

A.2.2 Serial number

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.1.2.2	Serial number of the certificate SHALL be a positive (non-negative) integer and It SHALL be unique for each certificate issued by a given CA. Serial number SHALL NOT be longer than 20 octets.

A.2.3 Signature

Referenced standard	Section	Requirement or recommendation

RFC 4055 [13]	5	pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)rsadsi(113549) pkcs(1) 1 }
		sha256WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 11}

A.2.4 Issuer

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.1.2.4	Conforming CAs "*MUST use either the PrintableString or UTF8String encoding of DirectoryString, with two exceptions. When CAs have previously issued certificates with issuer fields with attributes encoded using TeletexString, BMPString, or UniversalString, then the CA MAY continue to use these encodings of the DirectoryString to preserve backward compatibility*".
RFC 3739 [4]	3.1.1	*"The issuer field SHALL identify the organization responsible for issuing the certificate. The name SHOULD be an officially registered name of the organization"*.

A.2.5 Validity

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.1.2.5	*"CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later SHALL be encoded as GeneralizedTime"*.

A.2.6 Subject

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.1.2.6	Implementation requirements for this field are those defined for the issuer field (RFC 5280 [3] section 4.1.2.4).
RFC 3739 [4]	3.1.2	*"The countryName attribute value specifies a general context in which other attributes are to be understood. The country attribute does not necessarily indicate the subject's country of citizenship or country of residence, nor does it have to indicate the country of issuance. Many X.500 implementations require the presence of countryName in the DIT. In cases where the subject name, as specified in the subject field, specifies a public X.500 directory entry, the countryName attribute SHOULD always be present [...]* *It is the CA's responsibility to ensure that the serialNumber attribute is sufficient to resolve any subject name collisions"*.

A.2.7 Subject public key info

Referenced standard	Section	Requirement or recommendation

RFC 3279 [7]	2.3.1	The OID rsaEncryption identifies RSA public keys.
		pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)rsadsi(113549) pkcs(1) 1 }
		rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1}

A.3 X.509 version 2 certificate fields

No specific requirement listed.

A.4 Standard certificate extensions

A.4.1 Authority key identifier

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.2.1.1	*"The keyIdentifier field of the authorityKeyIdentifier extension MUST be included in all* end entity *certificates.* *The value of the keyIdentifier field SHOULD be derived from the public key used to verify the certificate's signature or a method that generates unique values.* *Two common methods for generating key identifiers from the public key are described in* RFC 5280 [3] (section 4.2.1.2)." This extension SHALL NOT be marked critical.
RFC 5280 [3]	4.2.1.2	*"The value of the subject key identifier in the parent CA certificate MUST be the value placed in the Authority Key Identifier extension of the* end entity *certificate"*.

A.4.2 Subject key identifier

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.2.1.2	This extension SHALL NOT be marked critical. To assist applications in identifying the appropriate end entity certificate, "*this extension MUST appear in all conforming CA certificates* [...] *and SHOULD be included in all end entity certificates*". *"Subject key identifiers SHOULD be derived from the public key or a method that generates unique values.* *Two common methods for generating key identifiers are:* *1) The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).* *2) The keyIdentifier is composed of a four bit type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING subjectPublicKey".*

A.4.3 KeyUsage

Referenced standard	Section	Requirement or recommendation
RFC 3739 [4]	3.2.4	*"The key usage extension SHALL be present*".
RFC 5280 [3]	4.2.1.3	When this extension appears, it SHOULD be marked critical.
RFC 3279 [7]	2.3.1	*"If the keyUsage extension is present in an end entity certificate which conveys an RSA public key, any combination of the following values MAY be present:* - *digitalSignature;* - *nonRepudiation;* - *keyEncipherment; and* - *dataEncipherment."*

A.4.4 Private key usage period

No specific requirements listed.

A.4.5 Certificate policies

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.2.1.4	*"When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }"*.
RFC 3739 [4]	3.2.3	*"The certificate policies extension SHALL contain the identifier of at least one certificate policy which reflects the practices and procedures undertaken by the CA.* *The certificate policy extension MAY be marked critical"*.

A.4.6 Policy mappings

No specific requirement listed.

A.4.7 Subject alternative name

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.1.2.6	*"Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name extension (section 4.2.1.6) to describe such identities"*.
RFC 5280 [3]	4.2.1.7	*"When the subjectAltName extension contains an Internet mail address, the address MUST be stored in the rfc822Name"*.

A.4.8 Issuer alternative name

No specific requirements listed.

A.4.9 Subject directory attributes

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.2.1.8	This extension SHALL be non-critical.

A.4.10 Basic constraints

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.2.1.9	*"This extension MAY appear as a critical or non-critical extension in end entity certificates"*.

A.4.11 Name constraints

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.2.1.10	The name constraints extension SHALL NOT be present in end entity certificates.

A.4.12 Policy constraints

No specific requirement listed.

A.4.13 Extended key usage

No specific requirement listed.

A.4.14 CRL distribution points

No specific requirement listed.

A.4.15 Inhibit any-policy

No specific requirement listed.

A.4.16 Freshest CRL

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.2.1.15	This extension SHALL be non-critical.

A.5 RFC 5280 internet certificate extensions

A.5.1 Authority information access

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.2.2.1	This extension SHALL be non-critical
RFC 2560 [11]	3.1	*"CAs that support an OCSP service, either hosted locally or provided by an Authorized Responder, MUST provide for the inclusion of a value for a uniformResourceIndicator (URI) accessLocation and the OID value id-ad-ocsp for the accessMethod in the AccessDescription SEQUENCE"*.

A.5.2 Subject information access

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.2.2.2	This extension SHALL be non-critical.

A.6 RFC 3739 certificate extensions

A.6.1 Biometric information

Referenced standard	Section	Requirement or recommendation
RFC 3739 [4]	3.2.5	This extension SHALL NOT be marked critical.

A.6.2 Qualified certificate statement

Referenced standard	Section	Requirement or recommendation
RFC 3739 [4]	3.2.6	*"This extension MAY be critical or non-critical. If the extension is critical, this means that all statements included in the extension are regarded as critical"*.

Annex B (normative):
Semantics identifier

Subject and names may include attributes that do not disclose the semantics of its information content. This is very common e.g. for information stored in the serialNumber attribute, which may contain a national identification number, passport number or any type of locally defined identifier. The semantics identifier, defined in RFC 3739 [4] offers one way to identify the type of information that is stored in various subject name fields and attributes.

RFC 3739 [4] section 3.2.6.1 defines the predefined statement "qcStatement-2" identified by the OID id-qcs-pkixQCSyntax-v2. This statement defines an optional semantics information field with the following structure:

```
SemanticsInformation ::= SEQUENCE {
    semanticsIdentifier        OBJECT IDENTIFIER   OPTIONAL,
    nameRegistrationAuthorities NameRegistrationAuthorities
                                                  OPTIONAL }
    (WITH COMPONENTS {..., semanticsIdentifier PRESENT}|
     WITH COMPONENTS {..., nameRegistrationAuthorities PRESENT})

NameRegistrationAuthorities ::=  SEQUENCE SIZE (1..MAX) OF
    GeneralName
```

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

This annex defines one optional semantics identifiers for inclusion in qcStatment-2 in the following clauses.

B.1 Natural person semantics identifier

Identifier:

```
id-etsi-qcs-SemanticsId-Natural     OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4)
etsi(0) id-natural-cert-profile(194122) 1 }
```

ASN.1 module:

```
ETSINaturalCprofile { itu-t(0) identified-organization(4) etsi(0) id-natural-cert-profile(194122)
id-mod(0) id-mod-natural-cert-profile(0) }


DEFINITIONS EXPLICIT TAGS::=

BEGIN

-- EXPORTS All --

-- Semantics identifier for natural person identifier

id-etsi-qcs-SemanticsId-Natural     OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4)
etsi(0) id-natural-cert-profile(194122) 1 }


END
```

Semantics definition:

When this 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 [15] country code.
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)).

- identifier (according to country and identity type reference).

The three initial characters have 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.

5) 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 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.

Annex C (informative): Change History

date	Version	Information about changes
July 2013	V1.1.2	Implemented Change Request: CR 01r1 in ESI(13)39_007r1 Error resolution – Illegal character in serialNumber
August 2013	V1.2.1	Publication

History

Document history		
V1.1.1	March 2004	Publication as TS 102 280
V1.1.1	April 2012	Publication
V1.2.1	August 2013	Publication