Draft ETSI EN 319 412-5 V2.2.0 (2017-08)

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

Reference
REN/ESI-0019412-5v221

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

Essential patents

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 (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 5 of multi-part deliverable covering the Certificates Profiles. Full details of the entire series can be found in part 1 [i.1].

The present document was previously published as ETSI TS 101 862 [i.4].

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

ITU and ISO issued standards for certification of public keys in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.7] which are used for the security of communications and data for a wide range of electronic applications.

The IETF qualified certificate profile, IETF RFC 3739 [2] defines an extension to X.509 certificates, the `qcStatements` extension, which can include statements relevant for qualified certificates. IETF RFC 3739 [2] defines qualified certificates in a general context as "a certificate whose primary purpose is to identify a person with a high level of assurance, where the certificate meets some qualification requirements defined by an applicable legal framework". The use of IETF RFC 3739 [2] `qcStatements` in the present document goes beyond the scope of the RFC which is directed at natural persons only.

The `qcStatements` certificate extension can contain any statement by the certificate issuer that can be useful to the relying party in determining the applicability of the certificate for an intended usage. Such statement can be a declaration that the certificate fulfils specific legal requirements for qualified certificates according to a defined legal framework.

The present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.8] Annexes I, III and IV.

1 Scope

The present document defines specific `QCStatement` for the `qcStatements` extension as defined in IETF RFC 3739 [2], clause 3.2.6, including requirements for their use in EU qualified certificates. Some of these `QCStatement`s can be used for other forms of certificate.

The `QCStatements` defined in the present document can be used in combination with any certificate profile, either defined in ETSI EN 319 412-2 [i.2], ETSI EN 319 412-3 [i.5] and ETSI EN 319 412-4 [i.6], or defined elsewhere.

The `QCStatements` defined in clause 4.3 may be applied to regulatory environments outside the EU. Other requirements specified in clause 4 are specific to Regulation (EU) No 910/2014 [i.8] but may be adapted for other regulatory environments.

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] ISO 639-1:2002: "Codes for the representation of names of languages -- Part 1: Alpha-2 code".

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

[3] Recommendation ITU-T X.680-X.699: "Information technology - Abstract Syntax Notation One (ASN.1)".

[4] ISO 4217: "Codes for the representation of currencies and funds".

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

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] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

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

[i.3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.4] ETSI TS 101 862: "Qualified Certificate profile".

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

[i.8] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.9] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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

[i.11] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

[i.12] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 319 412-1 [i.1] 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.8] or Annex I of the Directive 1999/93/EC [i.3] whichever is in force at the time of issuance

QCStatement: statement for inclusion in a qcStatements certificates extension as specified in IETF RFC 3739 [2]

qualified electronic signature/seal creation device: As specified in Regulation (EU) No 910/2014 [i.8].

secure signature creation device: As specified in Directive 1999/93 [i.3].

3.2 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
EC	European Commission
EU	European Union
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
PDS	PKI Disclosure Statements
PKI	Public Key Infrastructure
QC	Qualified Certificate
QSCD	Qualified electronic Signature/Seal Creation Device
RFC	Request For Comments
URL	Uniform Resource Locator

4 Qualified certificate statements

4.1 General requirements

The `qcStatements` extension shall be as specified in clause 3.2.6 of IETF RFC 3739 [2]. The `qcStatements` extension shall not be marked as critical.

The following clauses define a number of individual `QCStatements` to be included in the `qcStatements` extension.

The syntax of the defined statements shall comply with ASN.1 [3]. The complete ASN.1 module for all defined statements shall be as provided in Annex B; it takes precedence over the ASN.1 definitions provided in the body of the present document, in case of discrepancy.

NOTE: This extension is not processed as part of IETF RFC 5280 [i.9] path validation and there are no security implications with accepting a certificate in a system that cannot parse this extension.

4.2 `QCStatements` claiming compliance with the EU legislation

4.2.1 `QCStatement` claiming that the certificate is a EU qualified certificate

This `Qcstatement` claims that the certificate is an EU qualified certificate that is issued according to Directive 1999/93/EC [i.3] or the Annex I, III or IV of the Regulation (EU) No 910/2014 [i.8] whichever is in force at the time of issuance.

Syntax:

```
esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance }

id-etsi-qcs-QcCompliance      OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
```

The precise meaning of this statement is enhanced by the QC type statement defined in clause 4.2.3 according to the table 1.

Table 1: esi4-qcStatement-1 meaning

QC type statement (clause 4.2.3)	Meaning of this statement (`esi4-qcStatement-1`)
Absent	The certificate is issued according to Directive 1999/93/EC [i.3] or Annex I of the Regulation (EU) No 910/2014 [i.8] (for electronic signatures).
Present	The certificate is issued according to Annex I, III or IV of Regulation (EU) No 910/2014 [i.8] as of the types declared by the QC type statement in accordance with clause 4.2.3.

A certificate that includes this statement shall comply with all requirements defined in clause 5.

4.2.2 `QCStatement` claiming that the private key related to the certified public key resides in a QSCD

This `Qcstatement` declares that the private key related to the certified public key resides in a Qualified Signature/Seal Creation Device (QSCD) according to the Regulation (EU) No 910/2014 [i.8] or a secure signature creation device as defined in the Directive 1999/93/EC [i.3].

Syntax:

```
esi4-qcStatement-4 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcSSCD  }
```

```
id-etsi-qcs-QcSSCD  OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }
```

4.2.3 QCStatement claiming that the certificate is a EU qualified certificate of a particular type

This QCStatement declares that a certificate is issued as one and only one of the purposes of electronic signature, electronic seal or web site authentication.

This QCStatements states that an EU qualified certificate is issued as one specific types according to Annexes I, III or IV of the Regulation (EU) No 910/2014 [i.8] when used in combination with the qcStatement as defined in clause 4.2.1. When used on its own it indicates that it is used for the purposes of electronic signatures, seals or web sites for "non-qualified certificates" within the context of Regulation (EU) No 910/2014 [i.8].

NOTE: This statement, without the one defined in clause 4.2.1, can be potentially used in other regulatory environments which use electronic signature, electronic seal or web site with the same meaning.

Syntax:

```
esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED
 BY id-etsi-qcs-QcType }

Id-etsi-qcs-QcType      OBJECT IDENTIFIER ::= { id-etsi-qcs 6 }

 QcType::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-esign | id-etsi-qct-eseal |
                                          id-etsi-qct-web, ...)

-- QC type identifiers
id-etsi-qct-esign   OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 }
 -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014
id-etsi-qct-eseal  OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 }
 -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014
id-etsi-qct-web   OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }
 -- Certificate for website authentication as defined in Regulation (EU) No 910/2014
```

4.3 Generic QCStatements

4.3.1 Introduction

QCStatements defined in the following clauses may be used with any applicable regulatory framework.

4.3.2 QCStatement regarding limits on the value of transactions

This QCStatement declares a limitation on the value of transaction for which a certificate can be used.

Syntax:

```
esi4-qcStatement-2 QC-STATEMENT ::= { SYNTAX QcEuLimitValue IDENTIFIED
BY id-etsi-qcs-QcLimitValue }

QcEuLimitValue ::= MonetaryValue

MonetaryValue::= SEQUENCE {
    currency        Iso4217CurrencyCode,
    amount          INTEGER,
    exponent        INTEGER}
   -- value = amount * 10^exponent

 Iso4217CurrencyCode ::= CHOICE {
     alphabetic  PrintableString (SIZE (3)), -- Recommended
     numeric     INTEGER (1..999) }
     -- Alphabetic or numeric currency code as defined in ISO 4217
     -- It is recommended that the Alphabetic form is used

id-etsi-qcs-QcLimitValue      OBJECT IDENTIFIER ::= { id-etsi-qcs 2 }
```

The currency codes shall be as defined in ISO 4217 [4]. The alphabetic form should be used.

NOTE 1: This `QCStatement` was aimed at supporting Directive 1999/93/EC [i.3] which declared that qualified certificates could declare "limits on the value of transactions for which the certificate can be used, if applicable". The definition of EU qualified certificates according to the Regulation EU No 910/2014 [i.8] does not include any requirements on such declaration.

NOTE 2: It is outside the scope of this `QCStatement` to define how CA liability is affected by inclusion of this `QCStatement`. Relying parties can consult the certificate policy for further understanding of the implications of this statement.

4.3.3 `QCStatement` indicating the duration of the retention period of material information

Reliance on qualified certificates can depend on the existence of external information retained by the CA.

This `QCStatement` declares a retention period for material information relevant to the use of and reliance on a certificate, expressed as a number of years after the expiry date of the certificate.

Syntax:

```
esi4-qcStatement-3 QC-STATEMENT ::= { SYNTAX QcEuRetentionPeriod IDENTIFIED
BY id-etsi-qcs-QcRetentionPeriod }

QcEuRetentionPeriod ::= INTEGER

id-etsi-qcs-QcRetentionPeriod OBJECT IDENTIFIER ::= { id-etsi-qcs 3 }
```

NOTE: A significant aspect for an EU qualified certificate is that the Regulation (EU) No 910/2014 [i.8] allows name forms in certificates, such as pseudonyms, which can require assistance from the CA or a relevant name registration authority, in order to identify the associated physical person in case of a dispute.

4.3.4 `QCStatement` regarding location of PKI Disclosure Statements (PDS)

This `QCStatement` holds URLs to PKI Disclosure Statements (PDS) in accordance with Annex A of ETSI EN 319 411-1 [i.10].

Syntax:

```
esi4-qcStatement-5 QC-STATEMENT ::= { SYNTAX QcEuPDS IDENTIFIED
BY id-etsi-qcs-QcPDS }

QcEuPDS ::= PdsLocations

PdsLocations ::= SEQUENCE SIZE (1..MAX) OF PdsLocation

PdsLocation::= SEQUENCE {
    url        IA5String,
    language   PrintableString (SIZE(2))} --ISO 639-1 language code


id-etsi-qcs-QcPDS      OBJECT IDENTIFIER ::= { id-etsi-qcs 5 }
```

The language shall be as defined in ISO 639-1 [1].

Referenced PKI Disclosure Statements should be structured according to Annex A of ETSI EN 319 411-1 [i.10].

The signature of the certificate does not cover the content of the PDS and hence does not protect the integrity of the PDS which can change over time. End users trust in the accuracy of a PDS is therefore based on the mechanisms used to protect the authenticity of the PDS. As a minimum, a URL to a PDS provided in this statement shall use the "https" (https://) scheme, IETF RFC 2818 [5].

5 Requirements on QCStatements in EU qualified certificates

EU qualified certificates shall include QCStatements in accordance with table 2.

The column "Presence" contains the specification of the presence of the statement as follows:

- **M**: Mandatory. The statement shall be present.
- **O**: Optional. The statement may be present.

Table 2: Requirements on QCStatements

Clause	QCStatement	Presence	Additional requirements
4.2.1	esi4-qcStatement-1	M	
4.2.2	esi4-qcStatement-4	O	When the certificate is issued as a certificate where the private key related to the certified public key resides in a qualified signature/seal creation device in accordance with Regulation (EU) No 910/2014 [i.8] or in a secure signature creation device as defined in Directive 1999/93/EC [i.3], this statement shall be present.
4.2.3	esi4-qcStatement-6	O	When the certificate is issued in accordance with Annex III or Annex IV of Regulation (EU) No 910/2014 [i.8], this statement shall be present.
4.3.2	esi4-qcStatement-2	O	
4.3.3	esi4-qcStatement-3	O	
4.3.4	esi4-qcStatement-5	O	a) It shall provide at least one URL to a PDS in English. Other PDS documents in other languages may be referenced using this QCStatement provided that they provide information that corresponds to the information given in the referenced English PDS; and b) it shall not reference more than one PDS per language.

Annex A (informative): Relationship with the Regulation (EU) No 910/2014

A.1 EU qualified certificates for electronic signatures

Table A.1: Mapping with Annex I of the Regulation (EU) No 910/2014 [i.8]

Requirement from Annex I in the Regulation (EU) No 910/2014 [i.8]	Implementation according to the present document and referenced standards
(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;	Inclusion of QC statements defining this property as defined in clauses 4.2.1 and 4.2.3.
(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and: *- for a legal person: the name and, where applicable, registration number as stated in the official records,* *- for a natural person: the person's name;*	By information stored in the issuer field as defined in clause 4.2.3 of ETSI EN 319 412-2 [i.2].
(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;	As defined in clause 4.2.4 of ETSI EN 319 412-2 [i.2].
(d) electronic signature validation data that corresponds to the electronic signature creation data;	The public key with the associated information provided in the certificate according to IETF RFC 5280 [i.9] and further profiled in clause 4.2.5 of ETSI EN 319 412-2 [i.2].
(e) details of the beginning and end of the certificate's period of validity;	The validity period according to IETF RFC 5280 [i.9].
(f) the certificate identity code, which must be unique for the qualified trust service provider;	The serial number of the certificate according to IETF RFC 5280 [i.9].
(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;	The digital signature of the issuer according to IETF RFC 5280 [i.9].
(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;	Information provided in the Authority Info Access extension according to IETF RFC 5280 [i.9] and further profiled in clause 4.4.1 of ETSI EN 319 412-2 [i.2].
(i) the location of the services that can be used to enquire about the validity status of the qualified certificate;	Provided by information in the CRL Distribution point extension and/or the Authority Info Access extension according to IETF RFC 5280 [i.9] and further profiled in clauses 4.3.11 and 4.4.1 of ETSI EN 319 412-2 [i.2].
(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.	Inclusion of an explicit statement defining this property as defined in clause 4.2.2.

A.2 EU qualified certificates for electronic seals

Table A.2: Mapping with Annex III of the Regulation (EU) No 910/2014 [i.8]

Requirement from Annex III in the Regulation (EU) No 910/2014 [i.8]	Implementation according to the present document and referenced standards
(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;	Inclusion of QC statements defining this property as defined in clauses 4.2.1 and 4.2.3.
(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and: *- for a legal person: the name and, where applicable, registration number as stated in the official records,* *- for a natural person: the person's name;*	By information stored in the issuer field as defined in clause 4.2.3 of ETSI EN 319 412-2 [i.2].
(c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;	As defined in clause 4.2.1 of ETSI EN 319 412-3 [i.5].
(d) electronic seal validation data that corresponds to the electronic seal creation data;	The public key with the associated information provided in the certificate according to IETF RFC 5280 [i.9] and further profiled in clause 4.2.5 of ETSI EN 319 412-2 [i.2].
(e) details of the beginning and end of the certificate's period of validity;	The validity period according to IETF RFC 5280 [i.9].
(f) the certificate identity code, which must be unique for the qualified trust service provider;	The serial number of the certificate according to IETF RFC 5280 [i.9].
(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;	The digital signature of the issuer according to IETF RFC 5280 [i.9].
(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;	Information provided in the Authority Info Access extension according to IETF RFC 5280 [i.9] and further profiled in clause 4.4.1 of ETSI EN 319 412-2 [i.2].
(i) the location of the services that can be used to enquire about the validity status of the qualified certificate;	Provided by information in the CRL Distribution point extension and/or the Authority Info Access extension according to IETF RFC 5280 [i.9] and further profiled in clauses 4.3.11 and 4.4.1 of ETSI EN 319 412-2 [i.2].
(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.	Inclusion of an explicit statement defining this property as defined in clause 4.2.2.

A.3 EU qualified certificates for website authentication

Table A.3: Mapping with Annex IV of the Regulation (EU) No 910/2014 [i.8]

Requirement from Annex IV in the Regulation (EU) No 910/2014 [i.8]	Implementation according to the present document and referenced standards
(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;	Inclusion of an explicit statement defining this property as defined in clauses 4.2.1 and 4.2.3.
(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and: *- for a legal person: the name and, where applicable, registration number as stated in the official records,* *- for a natural person: the person's name;*	By information stored in the issuer field as defined in clause 7.1.4.1 of CA/Browser Forum Baseline Requirements [i.11].
(c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated; for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;	By information about the subject as defined in clause 7.1.4.2.2 of CA/Browser Forum Baseline Requirements [i.11] and clause 9.2.1 of CA/Browser Extended Validation Requirements [i.12].
(d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;	Information provided in the subject field in the certificate according to clause 7.1.4.2.2 of CA/Browser Forum Baseline Requirements [i.11] and clauses 9.2.5 and 9.2.7 of CA/Browser Extended Validation Requirements [i.12].
(e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;	Information provided in the dNSName subject alternative name and means as defined in clause 7.1.4.2.1 of CA/Browser Forum Baseline Requirements [i.11] and clause 9.2.2 of CA/Browser Extended Validation Requirements [i.12].
(f) details of the beginning and end of the certificate's period of validity;	The validity period according to IETF RFC 5280 [i.9].
(g) the certificate identity code, which must be unique for the qualified trust service provider;	The serial number of the certificate according to IETF RFC 5280 [i.9].
(h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;	The digital signature of the issuer according to IETF RFC 5280 [i.9].
(i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;	Information provided in the Authority Info Access extension according to IETF RFC 5280 [i.9] and further profiled in clause 7.1.2.3 c of CA/Browser Forum Baseline Requirements [i.11].
(j) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.	Provided by information in the CRL Distribution point extension and/or the Authority Info Access extension according to IETF RFC 5280 [i.9] and further profiled in clause 7.1.2.3 b and c of CA/Browser Forum Baseline Requirements [i.11] and clause 9.7 4) of CA/Browser Extended Validation Requirements [i.12].

Annex B (normative): ASN.1 declarations

```
ETSIQCstatementsMod { itu-t(0) identified-organization(4) etsi(0) id-qc-statements(194125) id-
mod(0) id-mod-qc-statements(0) }

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS All –

IMPORTS

QC-STATEMENT, qcStatement-2
     FROM PKIXqualified97 {iso(1) identified-organization(3) dod(6)
     internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
     id-mod-qualified-cert-97(35)};

-- statements

  -- EU qualified certificate declaration
  esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance }

  -- Declaration of limit value
  esi4-qcStatement-2 QC-STATEMENT ::= { SYNTAX QcEuLimitValue IDENTIFIED
  BY id-etsi-qcs-QcLimitValue }

    QcEuLimitValue ::= MonetaryValue

    MonetaryValue::= SEQUENCE {
       currency        Iso4217CurrencyCode,
       amount          INTEGER,
       exponent        INTEGER}
      -- value = amount * 10^exponent

    Iso4217CurrencyCode ::= CHOICE {
        alphabetic  PrintableString (SIZE (3)), -- Recommended
        numeric     INTEGER (1..999) }
        -- Alphabetic or numeric currency code as defined in ISO 4217
        -- It is recommended that the Alphabetic form is used

  -- Retention period declaration
  esi4-qcStatement-3 QC-STATEMENT ::= { SYNTAX QcEuRetentionPeriod IDENTIFIED
  BY id-etsi-qcs-QcRetentionPeriod }

    QcEuRetentionPeriod ::= INTEGER

  -- SSCD and QSCD declaration
  esi4-qcStatement-4 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcSSCD }

  -- PKI Disclosure statements
  esi4-qcStatement-5 QC-STATEMENT ::= { SYNTAX QcEuPDS IDENTIFIED
  BY id-etsi-qcs-QcPDS }

    QcEuPDS ::= PdsLocations

    PdsLocations ::= SEQUENCE SIZE (1..MAX) OF PdsLocation

    PdsLocation::= SEQUENCE {
       url        IA5String,
       language   PrintableString (SIZE(2))} --ISO 639-1 language code


  -- Certificate type
  esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED
  BY id-etsi-qcs-QcType }

  QcType::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-esign | id-etsi-qct-eseal |
                                           id-etsi-qct-web, ...)


-- object identifiers
id-etsi-qcs                  OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0)
id-qc-profile(1862) 1 }
```

```
id-etsi-qcs-QcCompliance        OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
id-etsi-qcs-QcLimitValue        OBJECT IDENTIFIER ::= { id-etsi-qcs 2 }
id-etsi-qcs-QcRetentionPeriod   OBJECT IDENTIFIER ::= { id-etsi-qcs 3 }
id-etsi-qcs-QcSSCD              OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }
id-etsi-qcs-QcPDS               OBJECT IDENTIFIER ::= { id-etsi-qcs 5 }
id-etsi-qcs-QcType              OBJECT IDENTIFIER ::= { id-etsi-qcs 6 }

-- QC type identifiers
id-etsi-qct-esign   OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 }
 -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014
id-etsi-qct-eseal  OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 }
 -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014
id-etsi-qct-web   OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }
 -- Certificate for website authentication defined in Regulation (EU) No 910/2014

-- supported statements

SupportedStatements QC-STATEMENT ::= {
    qcStatement-2 |
    esi4-qcStatement-1 | esi4-qcStatement-2 | esi4-qcStatement-3 |
    esi4-qcStatement-4 | esi4-qcStatement-5 | esi4-qcStatement-6, ...}

END
```

Annex C (informative): Change History

Date	Version	Information about changes
June 2017	2.2.0	CR002 (ESI(16)57_044) + ESI#59 modification Clause 4.2.3. First sentence modified to "This `QCStatement` declares that a certificate is issued as **one and only one of the purposes of electronic signature, electronic seal or web site authentication. This QCStatements states that an EU qualified certificate is issued as one** specific types according to Annexes I, III or IV of the Regulation (EU) No 910/2014 [i.8] when used in combination with the qcStatement as defined in clause 4.2.1."
June 2017	2.2.0	CR001 (ESI(17)58_008) Table 2: presence of `esi4-qcStatement-5` changed from M to O

History

Document history		
V1.1.1	December 2000	Publication as ETSI TS 101 862 (historical)
V1.2.1	June 2001	Publication as ETSI TS 101 862 (historical)
V1.3.1	March 2004	Publication as ETSI TS 101 862 (withdrawn)
V1.3.2	June 2004	Publication as ETSI TS 101 862 (historical)
V1.3.3	January 2006	Publication as ETSI TS 101 862 (historical)
V1.1.1	January 2013	Publication (withdrawn)
V2.0.13	July 2015	Publication as ETSI TS 119 412-5 (withdrawn)
V2.1.1	February 2016	Publication
V2.2.0	August 2017	EN Approval Procedure AP 20171121: 2017-08-23 to 2017-11-21