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

Intellectual Property Rights ................................................................................................................................ 4
Foreword ............................................................................................................................................................. 4
Modal verbs terminology .................................................................................................................................... 4
Introduction ........................................................................................................................................................ 5
1 Scope ............................................................................................................................................................. 6
2 References ................................................................................................................................................ 6
2.1 Normative references ................................................................................................................................. 6
2.2 Informative references ................................................................................................................................. 6
3 Definition of terms, symbols, abbreviations and notations ........................................................................... 7
3.1 Terms ............................................................................................................................................................ 7
3.2 Symbols ........................................................................................................................................................ 7
3.3 Abbreviations ............................................................................................................................................... 7
3.4 Notations .................................................................................................................................................... 8
4 Qualified certificate statements ................................................................................................................ 8
4.1 General requirements ................................................................................................................................ 8
4.2 QCStatements claiming compliance with specific legislation ...................................................................... 8
4.2.1 QCStatement claiming that the certificate is a EU qualified certificate or a certificate being qualified within a defined legal framework from an identified country or set of countries .................... 8
4.2.2 QCStatement claiming that the private key related to the certified public key resides in a QSCD .......... 9
4.2.3 QCStatement claiming that the certificate is a certificate of a particular type ......................................... 9
4.2.4 QCStatement stating the country or set of countries under the legislation of which the certificate is issued as a qualified certificate ......................................................................................... 9
4.3 Generic QCStatements ................................................................................................................................ 10
4.3.1 Introduction ............................................................................................................................................. 10
4.3.2 QCStatement regarding limits on the value of transactions ................................................................... 10
4.3.3 QCStatement indicating the duration of the retention period of material information ................................ 11
4.3.4 QCStatement regarding location of PKI Disclosure Statements (PDS) ................................................. 11
5 Requirements on QCStatements in EU qualified certificates .................................................................... 12
  A.1 EU qualified certificates for electronic signatures ...................................................................................... 13
  A.2 EU qualified certificates for electronic seals ............................................................................................. 14
  A.3 EU qualified certificates for website authentication ................................................................................ 15
Annex B (normative): ASN.1 declarations ...................................................................................................... 16
Annex C (informative): Change History ......................................................................................................... 18
History .............................................................................................................................................................. 19
Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. 3GPP™ and LTE™ are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 5 of multi-part deliverable covering the Certificate 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].

<table>
<thead>
<tr>
<th>National transposition dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of adoption of this EN:</td>
</tr>
<tr>
<td>Date of latest announcement of this EN (doa):</td>
</tr>
<tr>
<td>Date of latest publication of new National Standard or endorsement of this EN (dop/e):</td>
</tr>
<tr>
<td>Date of withdrawal of any conflicting National Standard (dow):</td>
</tr>
</tbody>
</table>

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 \texttt{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] \texttt{qcStatements} in the present document goes beyond the scope of the RFC which is directed at natural persons only.

The \texttt{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 QCStatements 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 can 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.


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”.


ETSI
3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 412-1 [i.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/EC [i.3].

3.2 Symbols

Void.

3.3 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
EC European Commission
EU European Union
3.4 Notations

For the purposes of the present document, the notations given in ETSI EN 319 412-1 [i.1] apply.

4 Qualified certificate statements

4.1 General requirements

QCS-4.1-01: The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739 [2].

QCS-4.1-02: 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.

QCS-4.1-03: The syntax of the defined statements shall comply with ASN.1 (Recommendations X.680 to X.683 [3]).

QCS-4.1-04: The complete ASN.1 module for all defined statements shall be as provided in Annex B. Annex B 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 specific legislation

4.2.1 QCStatement claiming that the certificate is a EU qualified certificate or a certificate being qualified within a defined legal framework from an identified country or set of countries

This QCStatement claims:

i) either 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; or

ii) that the certificate is a certificate that is issued as qualified within a defined legal framework from an identified country or set of countries.

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:

a) the QC type statement defined in clause 4.2.3 according to table 1; and
b) the QcCClegislation statement defined in clause 4.2.4 according to table 1A.

### Table 1: esi4-qcStatement-1 meaning

<table>
<thead>
<tr>
<th>QC type statement (esi4-qcStatement-6)</th>
<th>Meaning of this statement (esi4-qcStatement-1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absent</td>
<td>The certificate is issued for electronic signatures according to Directive 1999/93/EC [i.3] or to Annex I of the Regulation (EU) No 910/2014 [i.8], or in accordance with another regulatory environment which use electronic signature with the same meaning.</td>
</tr>
</tbody>
</table>
| Present                               | The certificate is issued:  
  • either 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; or  
  • according to another regulatory environment which use electronic signature, electronic seal or web site authentication with the same meaning. |

### Table 1A: esi4-qcStatement-1 meaning

<table>
<thead>
<tr>
<th>QcCClegislation statement (esi4-qcStatement-7)</th>
<th>Meaning of this statement (esi4-qcStatement-1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absent</td>
<td>The certificate is issued in accordance with Directive 1999/93/EC [i.3] or with Regulation (EU) No 910/2014 [i.8].</td>
</tr>
<tr>
<td>Present</td>
<td>The certificate is issued in accordance with the regulatory environment in application in the country or set of countries identified by the country code declared by the QcCClegislation statement in accordance with clause 4.2.4.</td>
</tr>
</tbody>
</table>

QCS–4.2.1-01: A certificate that includes the esi4-qcStatement-1 statement with the aim to declare that it 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:

a) shall not include the QcCClegislation statement; and

b) 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 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.

When used in combination with the qcStatement as defined in clause 4.2.1, this QCStatement states that a qualified certificate, within a specific legislative context, such as Regulation (EU) No 910/2014 [i.8], is issued as one and only one of the purposes of electronic signature, electronic seal or web site authentication.

When not used in combination with the qcStatement as defined in clause 4.2.1, it indicates that a certificate is issued as one and only one of the purposes of electronic signatures, seals or web site authentication for "non-qualified certificates" within a legislative context, which may be indicated by the qcStatement defined in clause 4.2.4.
EXAMPLE: This QCStatement states that an EU qualified certificate is issued as one specific type according to Annex 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 without the qcStatement defined in clause 4.2.4.

Syntax:

```plaintext
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
```

4.2.4QCStatement stating the country or set of countries under the legislation of which the certificate is issued as a qualified certificate

This QCStatement identifies the country or set of countries under the legislation of which the certificate is issued as a qualified certificate.

QCS-4.2.4-01: If the certificate is issued according to Directive 1999/93/EC [i.3] or the Regulation (EU) No 910/2014 [i.8], this QCStatement shall not be present.

Syntax:

```plaintext
esi4-qcStatement-7 QC-STATEMENT ::= { SYNTAX QcCClegislation IDENTIFIED BY id-etsi-qcs-QcCClegislation }

id-etsi-qcs-QcCClegislation OBJECT IDENTIFIER ::= { id-etsi-qcs 7 }

QcCClegislation ::= SEQUENCE OF CountryName

CountryName ::= PrintableString (SIZE (2)) (CONSTRAINED BY { -- ISO 3166-1 [6] alpha-2 codes only
-- })
```

4.3Generic QCStatements

4.3.1Introduction

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

4.3.2QCStatement 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:

```plaintext
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 }

QCS-4.3.2-01: The currency codes shall be as defined in ISO 4217 [4].

QCS-4.3.2-02: The alphabetic form of currency codes 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 }

QCS-4.3.4-01: The language shall be as defined in ISO 639-1 [1].

QCS-4.3.4-02: 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.
QCS-4.3.4-03: As a minimum, a URL to a PDS provided in this statement shall use the "https" (https://) scheme, IETF RFC 2818 [5] or later documents updating this specification.

5 Requirements on QCStatements in EU qualified certificates

QCS-5-01: 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.
- X: Forbidden. The statement shall not be present.

Table 2: Requirements on QCStatements

<table>
<thead>
<tr>
<th>Clause</th>
<th>QCStatement</th>
<th>Presence</th>
<th>Additional requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1</td>
<td>esi4-qcStatement-1</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>4.2.4</td>
<td>esi4-qcStatement-7</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>4.2.2</td>
<td>esi4-qcStatement-4</td>
<td>O</td>
<td>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.</td>
</tr>
<tr>
<td>4.2.3</td>
<td>esi4-qcStatement-6</td>
<td>O</td>
<td>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.</td>
</tr>
<tr>
<td>4.3.2</td>
<td>esi4-qcStatement-2</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>4.3.3</td>
<td>esi4-qcStatement-3</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>4.3.4</td>
<td>esi4-qcStatement-5</td>
<td>O</td>
<td>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.</td>
</tr>
</tbody>
</table>
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]

<table>
<thead>
<tr>
<th>Requirement from Annex I in the Regulation (EU) No 910/2014 [i.8]</th>
<th>Implementation according to the present document and referenced standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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;</td>
<td>Inclusion of QC statements defining this property as defined in clauses 4.2.1 and 4.2.3.</td>
</tr>
<tr>
<td>(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:</td>
<td>By information stored in the issuer field as defined in clause 4.2.3 of ETSI EN 319 412-2 [i.2].</td>
</tr>
<tr>
<td>- for a legal person: the name and, where applicable, registration number as stated in the official records,</td>
<td></td>
</tr>
<tr>
<td>- for a natural person: the person's name;</td>
<td></td>
</tr>
<tr>
<td>(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;</td>
<td>As defined in clause 4.2.4 of ETSI EN 319 412-2 [i.2].</td>
</tr>
<tr>
<td>(d) electronic signature validation data that corresponds to the electronic signature creation data;</td>
<td>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].</td>
</tr>
<tr>
<td>(e) details of the beginning and end of the certificate's period of validity;</td>
<td>The validity period according to IETF RFC 5280 [i.9].</td>
</tr>
<tr>
<td>(f) the certificate identity code, which must be unique for the qualified trust service provider;</td>
<td>The serial number of the certificate according to IETF RFC 5280 [i.9].</td>
</tr>
<tr>
<td>(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;</td>
<td>The digital signature of the issuer according to IETF RFC 5280 [i.9].</td>
</tr>
<tr>
<td>(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;</td>
<td>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].</td>
</tr>
<tr>
<td>(i) the location of the services that can be used to enquire about the validity status of the qualified certificate;</td>
<td>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].</td>
</tr>
<tr>
<td>(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.</td>
<td>Inclusion of an explicit statement defining this property as defined in clause 4.2.2.</td>
</tr>
</tbody>
</table>
### A.2 EU qualified certificates for electronic seals

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

<table>
<thead>
<tr>
<th>Requirement from Annex III in the Regulation (EU) No 910/2014 [i.8]</th>
<th>Implementation according to the present document and referenced standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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;</td>
<td>Inclusion of QC statements defining this property as defined in clauses 4.2.1 and 4.2.3.</td>
</tr>
<tr>
<td>(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:</td>
<td>By information stored in the issuer field as defined in clause 4.2.3 of ETSI EN 319 412-2 [i.2].</td>
</tr>
<tr>
<td>- for a legal person: the name and, where applicable, registration number as stated in the official records,</td>
<td></td>
</tr>
<tr>
<td>- for a natural person: the person’s name;</td>
<td></td>
</tr>
<tr>
<td>(c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;</td>
<td>As defined in clause 4.2.1 of ETSI EN 319 412-3 [i.5].</td>
</tr>
<tr>
<td>(d) electronic seal validation data that corresponds to the electronic seal creation data;</td>
<td>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].</td>
</tr>
<tr>
<td>(e) details of the beginning and end of the certificate’s period of validity;</td>
<td>The validity period according to IETF RFC 5280 [i.9].</td>
</tr>
<tr>
<td>(f) the certificate identity code, which must be unique for the qualified trust service provider;</td>
<td>The serial number of the certificate according to IETF RFC 5280 [i.9].</td>
</tr>
<tr>
<td>(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;</td>
<td>The digital signature of the issuer according to IETF RFC 5280 [i.9].</td>
</tr>
<tr>
<td>(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;</td>
<td>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].</td>
</tr>
<tr>
<td>(i) the location of the services that can be used to enquire about the validity status of the qualified certificate;</td>
<td>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].</td>
</tr>
<tr>
<td>(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;</td>
<td>Inclusion of an explicit statement defining this property as defined in clause 4.2.2.</td>
</tr>
</tbody>
</table>
## A.3 EU qualified certificates for website authentication

<table>
<thead>
<tr>
<th>Requirement from Annex IV in the Regulation (EU) No 910/2014 [i.8]</th>
<th>Implementation according to the present document and referenced standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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;</td>
<td>Inclusion of an explicit statement defining this property as defined in clauses 4.2.1 and 4.2.3.</td>
</tr>
<tr>
<td>(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:</td>
<td>By information stored in the issuer field as defined in clause 7.1.4.1 of CA/Browser Forum Baseline Requirements [i.11].</td>
</tr>
<tr>
<td>- for a legal person: the name and, where applicable, registration number as stated in the official records,</td>
<td></td>
</tr>
<tr>
<td>- for a natural person: the person’s name;</td>
<td></td>
</tr>
<tr>
<td>(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;</td>
<td>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].</td>
</tr>
<tr>
<td>(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;</td>
<td>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].</td>
</tr>
<tr>
<td>(e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;</td>
<td>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].</td>
</tr>
<tr>
<td>(f) details of the beginning and end of the certificate’s period of validity;</td>
<td>The validity period according to IETF RFC 5280 [i.9].</td>
</tr>
<tr>
<td>(g) the certificate identity code, which must be unique for the qualified trust service provider;</td>
<td>The serial number of the certificate according to IETF RFC 5280 [i.9].</td>
</tr>
<tr>
<td>(h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;</td>
<td>The digital signature of the issuer according to IETF RFC 5280 [i.9].</td>
</tr>
<tr>
<td>(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;</td>
<td>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].</td>
</tr>
<tr>
<td>(j) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.</td>
<td>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 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].</td>
</tr>
</tbody>
</table>
Annex B (normative):
ASN.1 declarations

ETSIQCStatementMod { itu-t(0) identified-organization(4) etsi(0) id-qc-statements(194125) id-mod(0) id-mod-qc-statements(0) v2(1)}

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, ...)

-- country or set of countries under the legislation of which the certificate is issued as a qualified certificate
esi4-qcStatement-7 QC-STATEMENT ::= { SYNTAX QcCCLegislation IDENTIFIED BY id-etsi-qcs-QcCCLegislation }
QC legislation ::= SEQUENCE OF CountryName
CountryName ::= PrintableString (SIZE (2)) (CONstrained BY { -- ISO 3166 alpha-2 codes only -- })

-- 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 }
id-etsi-qcs-QcCClegislation OBJECT IDENTIFIER ::= { id-etsi-qcs 7 }

-- 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 ::= {
cqStatement-2 |
  esi4-qcStatement-1 | esi4-qcStatement-2 | esi4-qcStatement-3 |
  esi4-qcStatement-4 | esi4-qcStatement-5 | esi4-qcStatement-6, esi4-qcStatement-7, ...}

END
Annex C (informative):
Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Information about changes</th>
</tr>
</thead>
</table>
| 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 QCStatement 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 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.                                                                                             |
| November 2017 | 2.2.1 | Publication.                                                                                                                                                  |
| October 2019 | 2.2.2 | CR004 (ESI(19)68_10r5
Clauses modified: 4.2 title, 4.2.1, 4.2.3, new clause 4.2.4, 5, Annex B
Extending the scope of QcCompliance statement for use by non-EU countries.                                                                 |
| December 2019 | 2.2.3 | Correction of module object identifier (v2 added) in Annex B
Final draft approved by remote consensus for submission to EN Approval Procedure.                                                                         |
| January 2020 | 2.2.3 | - Version sent to EN Approval Procedure
On https://docbox.etsi.org/esi/Open/Compared_deliverables, one will be able to see what changes have taken place between the previous published version (v2.2.1) and this version. |
| April 2023  |         | Updated to allocate reference number to each requirement in line with ETSI EN 319 411-1.                                                                  |
## History

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>V1.1.1</strong></td>
</tr>
<tr>
<td><strong>V1.2.1</strong></td>
</tr>
<tr>
<td><strong>V1.3.1</strong></td>
</tr>
<tr>
<td><strong>V1.3.2</strong></td>
</tr>
<tr>
<td><strong>V1.3.3</strong></td>
</tr>
<tr>
<td><strong>V1.1.1</strong></td>
</tr>
<tr>
<td><strong>V2.0.13</strong></td>
</tr>
<tr>
<td><strong>V2.1.1</strong></td>
</tr>
<tr>
<td><strong>V2.2.1</strong></td>
</tr>
<tr>
<td><strong>V2.3.1</strong></td>
</tr>
<tr>
<td><strong>V2.4.0</strong></td>
</tr>
<tr>
<td><strong>V2.4.1</strong></td>
</tr>
</tbody>
</table>