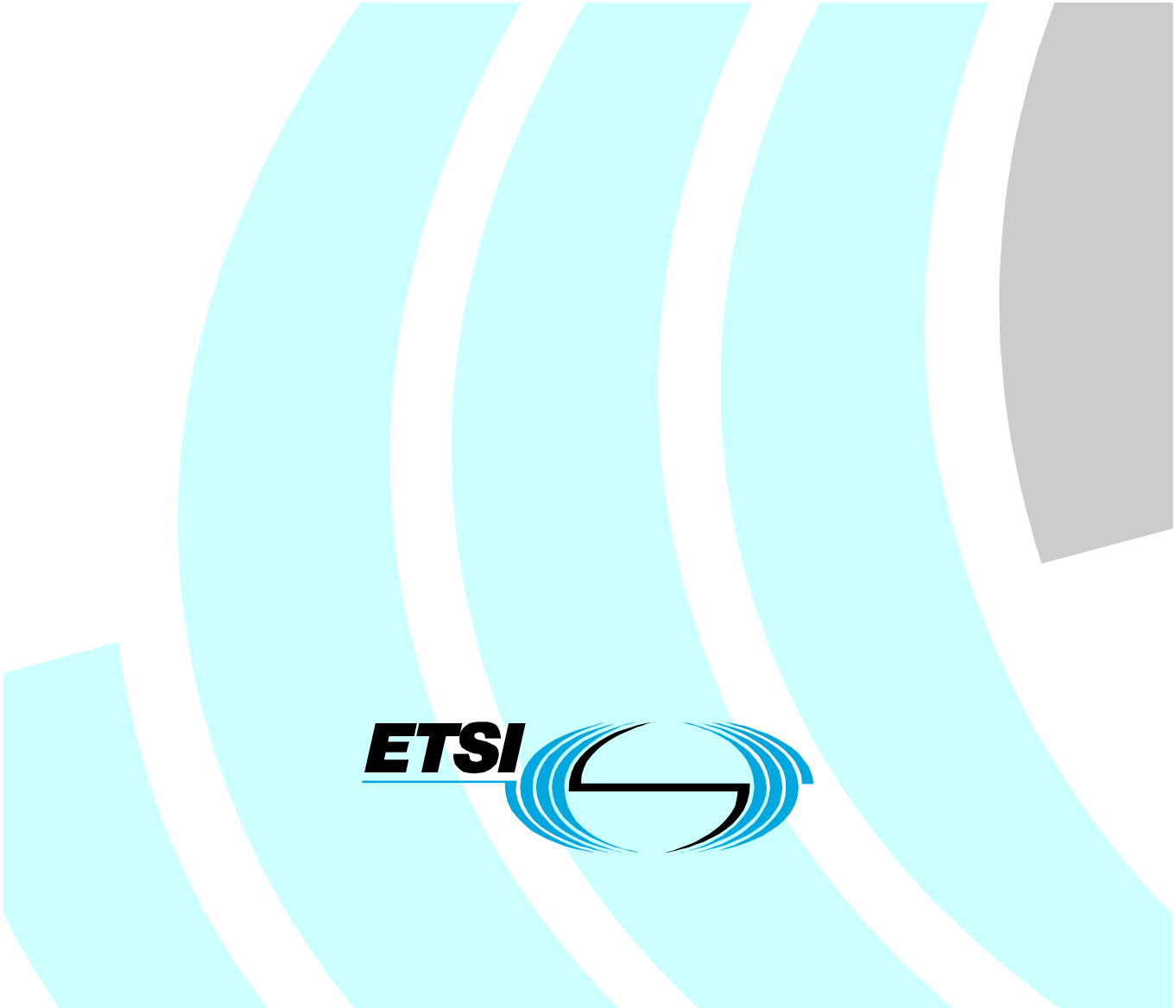
ETSI TS 101 862 V1.3.2 (2004-06)

Technical Specification

Qualified Certificate profile



Reference
RTS/ESI-000032

Keywords
electronic signature, IP, 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

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://webapp.etsi.org/IPR/home.asp).

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).

Introduction

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". These certificates are given a specific relevance for acceptance of electronic signatures through the following part of article 5 (Legal effects of electronic signatures):

Member States shall ensure that advanced electronic signatures which are based on a Qualified Certificate and which are created by a secure-signature-creation device:

a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

b) are admissible as evidence in legal proceedings.

The Directive 1999/93/EC [1] defines a Qualified Certificate in article 2 as:

- ""Qualified Certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II".

1 Scope

The present document defines a profile for Qualified Certificates, based on the technical definitions in RFC 3739 [4], that may be used by issuers of Qualified Certificates complying with Annex I and II of the European Electronic Signature Directive 1999/93/EC [1].

This Qualified Certificate profile and the IETF Qualified Certificate profile RFC 3739 [4] address Qualified Certificates within different contexts and therefore also use the term Qualified Certificate with slightly different meanings. While the IETF profile uses the term Qualified Certificates within a universal context independent of local legal requirements, this profile uses the term to explicitly describe a Qualified Certificate as defined in the European Electronic Signature Directive 1999/93/EC [1].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

[3] IETF RFC 3280: "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] ISO/IEC 8824-1/ITU-T Recommendation X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[6] ISO/IEC 8824-2/ITU-T Recommendation X.681: "Information technology - Abstract Syntax Notation One (ASN.1): Information object specification".

[7] ISO/IEC 8824-3/ITU-T Recommendation X.682: "Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification".

[8] ISO/IEC 8824-4/ITU-T Recommendation X.683: "Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications".

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

3 Abbreviations

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

CA	Certification Authority
OID	Object Identifier
SSCD	Secure Signature Creation Device

4 Document structure

The normative and informative parts of the present document are provided according to the following document structure:

- clause 4 contains the core part of the present document, defining the amendments to RFC 3739 [4];
- annex A provide a general information how the requirements of Annex I of the Directive can be implemented using tools defined in the present document as well as tools in the underlying standards RFC 3280 [3] and ITU-T Recommendation X.509 [2];
- annex B contains the ASN.1 (ISO/IEC 8824-1 [5], ISO/IEC 8824-2 [6], ISO/IEC 8824-3 [7], ISO/IEC 8824-4 [8]) modules of the present document.

5 Certificate Profile

This profile is based on the Internet certificate profile RFC 3739 [4], which in turn is based on RFC 3280 [3] and the X.509 version 3 [2]. For full implementation of this profile, implementers are REQUIRED to consult the underlying formats and semantics defined in RFC 3739 [4].

In case of discrepancies between the present document and RFC 3739 [4], the present document is the normative one.

5.1 Issuer field

The name of the issuer contained in the issuer field (as defined in clause 3.1.1 in RFC 3739 [4]) MUST contain a country name stored in the `countryName` attribute. The specified country SHALL be the country in which the issuer of the certificate is established.

5.2 Qualified Certificate Statements

This profile defines a number of individual statements for use with the extension for Qualified Certificates Statements "`qCStatements` extension", defined in RFC 3739 [4].

When this extension is marked critical, this means that all statements included in the extension are regarded as critical.

The following statements are defined in this profile:

- statement claiming that the certificates is issued as a Qualified Certificate;
- statement regarding limits on the value of transactions for which the certificate can be used;
- statement indicating the duration of the retention period during which registration information is archived;
- statement claiming that the private key associated with the public key in the certificate resides within a Secure Signature Creation Device.

5.2.1 Statement claiming that the certificates is a Qualified Certificate

The statement defined in this clause contains:

- An Identifier of the statement (represented by an OID) made by the CA, stating that this certificate is issued as a Qualified Certificate according to Annex I and II of the EU Directive 1999/93/EC [1], as implemented in the law of the country where the CA is established.

```
  esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED
  BY id-etsi-qcs-QcCompliance }
  --  This statement is a statement by the issuer that this
  --  certificate is issued as a Qualified Certificate according
  --  Annex I and II of the Directive 1999/93/EC of the European Parliament
  --  and of the Council of 13 December 1999 on a Community framework
  --  for electronic signatures, as implemented in the law of the country
  --  specified in the issuer field of this certificate.

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

5.2.2 Statement regarding limits on the value of transactions

The limits on the value of transactions, for which the certificate can be used, if applicable, may be indicated using the statement defined in this clause. The codes are defined in ISO 4217 [9].

This optional statement contains:

- an identifier of this statement (represented by an OID);
- a monetary value expressing the limit on the value of transactions.

```
   esi4-qcStatement-2 QC-STATEMENT ::= { SYNTAX QcEuLimitValue IDENTIFIED
   BY id-etsi-qcs-QcLimitValue }
   --  This statement is a statement by the issuer which impose a
   --  limitation on the value of transaction for which this certificate
   --  can be used to the specified amount (MonetaryValue), according to
   --  the Directive 1999/93/EC of the European Parliament and of the
   --  Council of 13 December 1999 on a Community framework for
   --  electronic signatures, as implemented in the law of the country
   --  specified in the issuer field of this certificate.

   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 }
```

5.2.3 Statement indicating the duration of the retention period of material information

Reliance on Qualified Certificates may depend on the existence of external information retained by the CA. A significant aspect is that the Directive 1999/93/EC [1] allows name forms in certificates, such as pseudonyms, which may require assistance from the CA or a relevant name registration authority, in order to identify the associated physical person in case of a dispute.

This optional statement contains:

- an identifier of this statement (represented by an OID);
- a retention period for material information relevant to the use of and reliance on the certificate, expressed as a number of years after the expiry date of the certificate.

```
   esi4-qcStatement-3 QC-STATEMENT ::= { SYNTAX QcEuRetentionPeriod IDENTIFIED
   BY id-etsi-qcs-QcRetentionPeriod }
   --  This statement is a statement by which the issuer guarantees
   --  that for the certificate where this statement appears that
   --  material information relevant to use of and reliance on the certificate
   --  will be archived and can be made available upon
   --  request beyond the end of the validity period of the certificate
   --  for the number of years as indicated in this statement.

   QcEuRetentionPeriod ::= INTEGER

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

5.2.4 Statement claiming that the private key related to the certified public key resides in a Secure Signature Creation Device

CAs claiming to issue certificates where the private key related to the certified public key resides in a Secure Signature Creation Device (SSCD) MAY use this optional statement. This optional statement contains:

- An Identifier of the statement (represented by an OID), made by the CA, stating that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device according to Annex III of the EU Directive 1999/93/EC [1], as implemented in the law of the country where the CA is established.

```
   esi4-qcStatement-4 QC-STATEMENT ::= { SYNTAX QcSSCD IDENTIFIED
   BY id-etsi-qcs-QcSSCD }
   --  This statement is a statement by which the issuer claims
   --  that for the certificate where this statement appears
   --  the private key associated with the public key in the certificate
   --  is protected according to Annex III of the Directive 1999/93/EC of
   --  the European Parliament and of the Council of 13 December 1999 on a
   --  Community framework for electronic signatures.

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

5.3 Qualified Certificate Indication

The following two techniques can be utilized to declare that a certificate is issued as a Qualified Certificate:

1) by identifying a certificate policy in the Certificate Policies extensions, as defined in clause 4.2.1.5 from RFC 3280 [3], clearly expressing that the issuer intentionally has issued the certificate as a Qualified Certificate and that the issuer claims compliance with annex I and annex II of the Directive [1]; or

2) by including a Qualified Certificate Statements extension with an esi4-qcStatement-1 statement as defined in clause 5.2.1 of this profile.

Qualified Certificates compliant with this specification SHOULD include a policy according to 1).

Qualified Certificates compliant with this specification issued **until** June 30, 2005 SHOULD contain a statement according to 2). Qualified Certificates compliant with this specification issued **after** June 30, 2005 SHALL contain a statement according to 2).

Qualified Certificates compliant with this specification SHALL in any case use at least one of the techniques 1) or 2) above.

Annex A (informative): Relationship with the Directive

Annex A describes how requirements from the Directive are addressed by the present document and referenced standards.

A.1 Annex I of the Directive

Table A.1: Annex I of the Directive

	Requirement from Annex I in the Directive 1999/93/EC [1]	Implementation according to this profile and underlying standards
(a)	an indication that the certificate is issued as a Qualified Certificate;	Inclusion of certificate policy defining this property and/or an explicit statement defining this property as defined in clause 5.3.
(b)	the identification of the certification-service-provider and the State in which it is established;	By information stored in the issuer field as defined in clause 3.1.1 of the IETF Qualified Certificate Profile RFC 3739 [4]. The certificate must clearly indicate the country in which the issuer is established as defined in clause 5.1.
(c)	the name of the signatory or a pseudonym, which shall be identified as such;	As defined in clause 3.1.2 of the IETF Qualified Certificate Profile RFC 3739 [4].
(d)	provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;	As defined in clauses 3.1.2 and 3.2.1 of the IETF Qualified Certificate Profile RFC 3739 [4].
(e)	signature-verification data which correspond to signature-creation data under the control of the signatory;	The public key with the associated information listed in annex A.
(f)	an indication of the beginning and end of the period of validity of the certificate;	The validity period according to ITU-T Recommendation X.509 [2] and RFC 3280 [3].
(g)	the identity code of the certificate;	The serial number of the certificate according to ITU-T Recommendation X.509 [2] and RFC 3280 [3].
(h)	the advanced electronic signature of the certification-service-provider issuing it;	The digital signature of the issuer according to ITU-T Recommendation X.509 [2] and RFC 3280 [3].
(i)	limitations on the scope of use of the certificate, if applicable; and	Provided by information in the certificate Policies extension, the Key Usage Extension and the Extended Key Usage Extension according to ITU-T Recommendation X.509 [2] and RFC 3280 [3].
(j)	limits on the value of transactions for which the certificate can be used, if applicable.	According to clause 5.2.2 of the present document.

A.2 Annex II of the Directive

Annex II contains "requirements for certification-service-providers issuing Qualified Certificates", which generally do not impact certificate format. Some specific functions of Qualified Certificates, as listed below, may however be used to support some of these requirements.

Table A.2: Annex II of the Directive

Requirement from Annex II in the Directive 1999/93/EC [1]	Supporting mechanisms
Requirement b) includes requirement on a secure and immediate revocation service.	The certificate extensions CRL distribution point and authority information access according to RFC 3280 [3] may contain information used to find and identify these services.
Requirement i) includes requirement on retention of relevant information for an appropriate period of time.	Clause 5.2.3 defines a statement that can be used to communicate the retention period to relying parties.
Requirement k) states that relevant part of the terms and conditions regarding the use of the certificate shall be made available on request to third-parties relying on the certificate.	A certificate policy identified in the certificate policies extension may contain a qualifier of the type "CPSuri", according to RFC 3280 [3], pointing to the location where such information can be obtained.

Annex B (normative): ASN.1 declarations

```
ETSIQCprofile { itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) id-mod(0) id-mod-qc-
profile-2(02) }

DEFINITIONS EXPLICIT TAGS::=

BEGIN

-- EXPORTS All --

IMPORTS

QC-STATEMENT, qcStatement-1
     FROM PKIXqualified93 {iso(1) identified-organization(3) dod(6)
     internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
     id-mod-qualified-cert-93(11)};

-- statements

  esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED
  BY id-etsi-qcs-QcCompliance }
  --  This statement is a statement by the issuer that this
  --  certificate is issued as a Qualified Certificate according
  --  Annex I and II of the Directive 1999/93/EC of the European Parliament
  --  and of the Council of 13 December 1999 on a Community framework
  --  for electronic signatures, as implemented in the law of the country
  --  specified in the issuer field of this certificate.

   esi4-qcStatement-2 QC-STATEMENT ::= { SYNTAX QcEuLimitValue IDENTIFIED
   BY id-etsi-qcs-QcLimitValue }
   --  This statement is a statement by the issuer which impose a
   --  limitation on the value of transaction for which this certificate
   --  can be used to the specified amount (MonetaryValue), according to
   --  the Directive 1999/93/EC of the European Parliament and of the
   --  Council of 13 December 1999 on a Community framework for
   --  electronic signatures, as implemented in the law of the country
   --  specified in the issuer field of this certificate.

   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

   esi4-qcStatement-3 QC-STATEMENT ::= { SYNTAX QcEuRetentionPeriod IDENTIFIED
   BY id-etsi-qcs-QcRetentionPeriod }
   --  This statement is a statement by which the issuer guarantees
   --  that for the certificate where this extension appears that the
   --  information received from the subscriber at the time of
   --  registration will be archived and can be made available upon
   --  request beyond the end of the validity period of the certificate
   --  for the number of years as indicated in this statement.

   QcEuRetentionPeriod ::= INTEGER

   esi4-qcStatement-4 QC-STATEMENT ::= { SYNTAX QcSSCD IDENTIFIED
   BY id-etsi-qcs-QcSSCD }
   --  This statement is a statement by which the issuer claims
   --  that for the certificate where this statement appears that
   --  the private key associated with the public key in the certificate
   --  is protected according to Annex III of the Directive 1999/93/EC of
   --  the European Parliament and of the Council of 13 December 1999 on a
   --  Community framework for electronic signatures.
```

```
-- 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 }

-- supported statements

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

END
```

History

Document history		
V1.1.1	December 2000	Publication
V1.2.1	June 2001	Publication
V1.3.1	March 2004	Publication (Withdrawn)
V1.3.2	June 2004	Publication