This document is meant purely as a documentation tool and the institutions do not assume any liability for its contents

►B ►C1 **COMMISSION DECISION**

of 16 October 2009

setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market

(notified under document C(2009) 7806)

(Text with EEA relevance)

(2009/767/EC) ◄

(OJ L 274, 20.10.2009, p. 36)

Amended by:

		Official Journal		
		No	page	date
►M1	Commission Decision 2010/425/EU of 28 July 2010	L 199	30	31.7.2010
►M2	Commission Regulation (EU) No 519/2013 of 21 February 2013	L 158	74	10.6.2013

Corrected by:

►C1	Corrigendum, OJ L 299, 14.11.2009, p. 18 (2009/767/EC)

▼B
▼C1

COMMISSION DECISION

of 16 October 2009

setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market

(notified under document C(2009) 7806)

(Text with EEA relevance)

(2009/767/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market [1], and in particular Article 8(3) thereof,

Whereas:

(1) The obligations of administrative simplification imposed on Member States in Chapter II of Directive 2006/123/EC, in particular Articles 5 and 8 thereof, include the obligation to simplify the procedures and formalities applicable to the access to and exercise of a service activity and the obligation to ensure that those procedures and formalities may be easily completed by service providers at a distance and by electronic means through the 'points of single contact'.

(2) The completion of procedures and formalities through the 'points of single contact' must be possible across borders between Member States as set out in Article 8 of Directive 2006/123/EC.

(3) To comply with the obligation to simplify procedures and formalities and to facilitate the cross-border use of the 'points of single contact', procedures by electronic means should rely on simple solutions, including as regards the use of electronic signatures. In cases where, after an appropriate risk assessment of concrete procedures and formalities, a high level of security or equivalence to a handwritten signature is deemed to be necessary, advanced electronic signatures based on a qualified certificate, with or without a secure signature creation device, could be required from service providers for certain procedures and formalities.

[1] OJ L 376, 27.12.2006, p. 36.

▼C1

(4) The Community framework for e-signatures was established in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures ([1]). In order to facilitate effective cross-border use of advanced electronic signatures based on a qualified certificate, trust in these electronic signatures should be enhanced irrespective of the Member State in which the signatory or the certification service provider issuing the qualified certificate is established. This could be achieved by making the information necessary to validate the electronic signatures more easily available in a trustworthy form, in particular information relating to certification service providers who are supervised/accredited in a Member State and to the services they offer.

(5) It is necessary to ensure that Member States make this information publicly available through a common template in order to facilitate its use and ensure an appropriate level of detail allowing the receiving side to validate the electronic signature,

HAS ADOPTED THIS DECISION:

Article 1

Use and acceptance of electronic signatures

1. If justified on the basis of an appropriate assessment of the risks involved and in accordance with Article 5(1) and (3) of Directive 2006/123/EC, Member States may require, for the completion of certain procedures and formalities through the points of single contact under Article 8 of Directive 2006/123/EC, the use by the service provider of advanced electronic signatures based on a qualified certificate, with or without a secure-signature-creation device, as defined and governed by Directive 1999/93/EC.

2. Member States shall accept any advanced electronic signature based on a qualified certificate, with or without a secure-signature-creation device, for the completion of the procedures and formalities referred to in paragraph 1, without prejudice to the possibility for Member States to limit this acceptance to advanced electronic signatures based on a qualified certificate and created by a secure-signature-creation device if this is in accordance with the risk assessment referred to in paragraph 1.

3. Member States shall not make the acceptance of advanced electronic signatures based on a qualified certificate, with or without a secure-signature-creation device, subject to requirements which create obstacles to the use, by service providers, of procedures by electronic means through the points of single contact.

([1]) OJ L 13, 19.1.2000, p. 12.

▼C1

4. Paragraph 2 does not prevent Member States from accepting electronic signatures other than advanced electronic signatures based on a qualified certificate, with or without a secure-signature-creation device.

Article 2

Establishment, maintenance and publication of trusted lists

1. Each Member State shall establish, maintain and publish, in accordance with the technical specifications set out in the annex, a 'trusted list' containing the minimum information related to the certification service providers issuing qualified certificates to the public who are supervised/accredited by them.

▼M1

2. Member States shall establish and publish both a human readable and a machine processable form of the trusted list in accordance with the specifications set out in the Annex.

2a. Member States shall sign electronically the machine processable form of their trusted list and they shall, as a minimum, publish the human readable form of the trusted list through a secure channel in order to ensure its authenticity and integrity.

3. Member States shall notify to the Commission the following information:

(a) the body or bodies responsible for the establishment, maintenance and publication of the human readable and machine processable forms of the trusted list;

(b) the locations where the human readable and machine processable forms of the trusted list are published;

(c) the public key certificate used to implement the secure channel through which the human readable form of the trusted list is published or, if the human readable list is electronically signed, the public key certificate used to sign it;

(d) the public key certificate used to electronically sign the machine processable form of the trusted list;

(e) any changes to the information in points (a) to (d).

4. The Commission shall make available to all Member States, through a secure channel to an authenticated web server, the information, referred to in paragraph 3, as notified by Member States, both in a human readable form and in a signed machine processable form.

▼C1

Article 3

Application

This Decision shall apply from 28 December 2009.

Article 4

Addressees

This Decision is addressed to the Member States.

▼C1

ANNEX

TECHNICAL SPECIFICATIONS FOR A COMMON TEMPLATE FOR THE 'TRUSTED LIST OF SUPERVISED/ACCREDITED CERTIFICATION SERVICE PROVIDERS'

PREFACE

1. **General**

The purpose of the Common Template for Member States' 'Trusted List of supervised/accredited Certification Service Providers' is to establish a common way in which information is provided by each Member State about the supervision/accreditation status of the certification services from Certification Service Providers ([1]) (CSPs) who are supervised/accredited by them for compliance with the relevant provisions of Directive 1999/93/EC. This includes the provision of historical information about the supervision/accreditation status of the supervised/accredited certification services.

The mandatory information in the Trusted List (TL) must include a minimum of information on supervised/accredited CSPs issuing Qualified Certificates (QCs) ([2]) in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3,3, 3,2, and Art 7.1(a)), including information on the QC supporting an electronic signature and whether or not the signature is created by a Secure Signature Creation Device (SSCD) ([3]).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List at a national level on a voluntary basis.

This information is aimed primarily at supporting the validation of Qualified Electronic Signatures (QES) and Advanced Electronic Signatures (AdES) ([4]) supported by a Qualified Certificate ([5]) ([6]).

The proposed Common Template is compatible with an implementation based on the specifications from ETSI TS 102 231 ([7]) that are used to address the establishment, publication, location, access, authentication and trusting of such kinds of lists.

([1]) As defined in Art. 2,11 of Directive 1999/93/EC.
([2]) As defined in Art. 2,10 of Directive 1999/93/EC.
([3]) As defined in Art. 2,6 of Directive 1999/93/EC.
([4]) As defined in Art. 2,2 of Directive 1999/93/EC.
([5]) For an AdES supported by a QC the acronym '$AdES_{QC}$' is used throughout the present document.
([6]) Note that there are a number of electronic services based on simple AdES whose cross-border use would also be facilitated, provided that the supporting certification services (e.g. issuing of non-qualified certificates) are part of the supervised/accredited services covered by a Member State in the voluntary information part of their Trusted List.
([7]) ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

2. **Guidelines for editing entries in the TL**

2.1. *A TL focusing on supervised/accredited certification services*

Relevant Certification Services and Certification Service Providers in a single List

The Trusted List of a Member State is defined as the 'Supervision/Accreditation Status List of certification services from Certification Service Providers who are supervised/accredited by the referenced Member State for compliance with the relevant provisions of Directive 1999/93/EC'.

Such a Trusted List must cover:

— **all Certification Service Providers**, as defined in Article 2.11 of Directive 1999/93/EC, i.e. 'entity or a legal or natural person who issues certificates or provides other services related to electronic signatures';

— **that are supervised/accredited** for compliance with the relevant provisions laid down in Directive 1999/93/EC.

When considering the definitions and provisions laid down in Directive 1999/93/EC, in particular with regard to the relevant CSPs and their supervision/voluntary accreditation systems, two sets of CSPs can be distinguished, namely the CSPs issuing QCs to the public (CSP_{QC}), and the CSPs not issuing QCs to the public but providing 'other (ancillary) services related to electronic signatures':

— **CSPs issuing QCs:**

  — They must be supervised by the Member State in which they are established (if they are established in a Member State) and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State.

  — The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3,3, Art. 8,1, Art. 11, recital (13) (respectively, Art.2.13, Art. 3,2, Art 7.1(a), Art. 8,1, Art. 11, recitals (4)-(11-13)).

— **CSPs not issuing QCs:**

  — They may fall under a 'voluntary accreditation' system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined 'recognised approval scheme' implemented on a national basis for the supervision of compliance with the provisions laid down in the Directive and possibly with national provisions with regard to the provision of certification services (in the sense of Art. 2,11 of the Directive).

  — Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to a specific 'qualification' on the basis of their compliance with the provisions and requirements laid down at national level, but the meaning of such a 'qualification' is likely to be limited solely to the national level.

▼C1

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates to the public in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3,3, 3,2 and Art. 7.1(a)), information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

Additional information on other supervised/accredited services from CSPs not issuing QCs to the public (e.g. CSPs providing Time Stamping Services and issuing Time Stamp Tokens, CSPs issuing non-Qualified certificates, etc.) may be included in the Trusted List at national level on a voluntary basis.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by the Member State responsible for establishing and maintaining the List for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— facilitating the validation of electronic signatures supported by the listed supervised/accredited certification services from the listed CSPs.

A single set of Supervision/Accreditation status values

One single TL must be established and maintained per Member State to indicate the supervision and/or accreditation status of those certification services from those CSPs that are supervised/accredited by the Member State.

The fact that a service is currently either supervised or accredited is part of its current status. In addition to that, a supervision or accreditation status can be 'ongoing', 'in cessation', 'ceased', or even 'revoked'. Throughout its lifetime, the same certification service may move from a supervision status to an accreditation status and vice versa ([1]).

The following Figure 1 describes the expected flow, for one single certification service, between possible supervision/accreditation statuses:

([1]) E.g. a certification service provider established in a Member State that provides a certification service that is initially supervised by the Member State (Supervisory Body), can, after a certain time, decide to pass a voluntary accreditation for the currently supervised certification service. Conversely, a certification service provider in another Member State can decide not to stop an accredited certification service but to move it from an accreditation status to a supervision status, e.g. for business and/or economic reasons.

▼C1

Expected supervision/accreditation status flow for a single CSP service

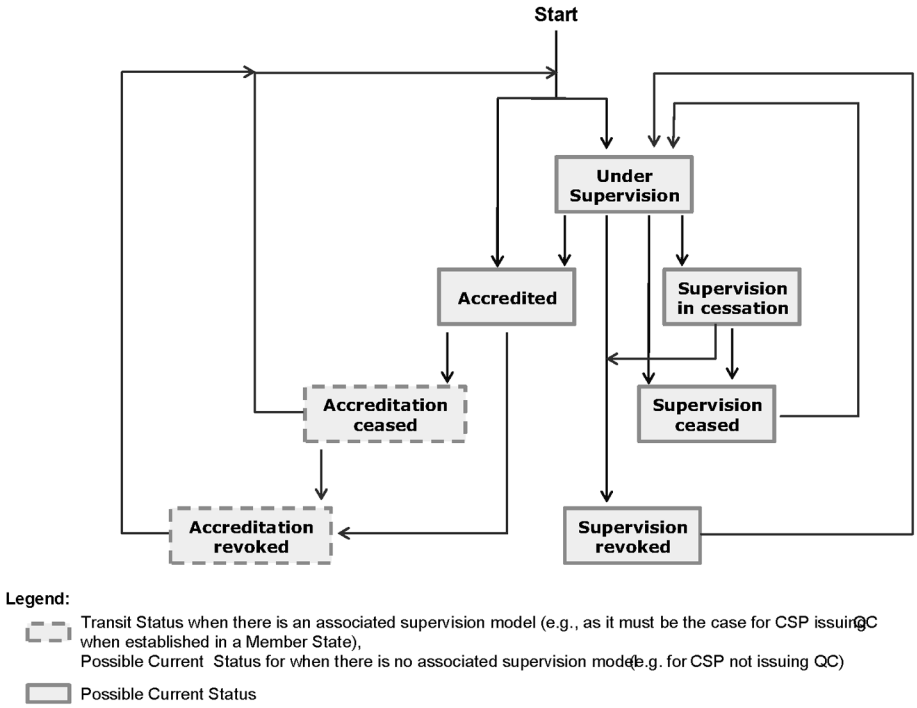


Figure 1

A certification service issuing QCs must be supervised (if it is established in a Member State) and may be voluntarily accredited. The status value of such a service when listed in a Trusted List can have any of the above depicted status values as 'current status value'. However, it should be noted that 'Accreditation ceased' and 'Accreditation revoked' must both be 'transit status' values only in the case of CSP_{QC} services established in a Member State, as such services must be supervised by default (even when not or no longer accredited).

It is required that Member States establishing or having established a nationally defined 'recognised approval scheme(s)' implemented on a national basis for the supervision of compliance of services from CSPs not issuing QCs with the provisions laid down in Directive 1999/93/EC and with possible national provisions with regard to the provision of certification services (in the sense of Art. 2,11 of the Directive) will categorise such approval scheme(s) under the following two categories:

— 'voluntary accreditation' as defined and regulated in Directive 1999/93/EC (Art.2.13, Art. 3,2, Art 7.1(a), Art. 8,1, Art. 11, recitals (4)-(11-13));

— 'supervision' as required in Directive 1999/93/EC and implemented by national provisions and requirements in accordance with national laws.

▼C1

Accordingly, a certification service not issuing QCs may be supervised or voluntarily accredited. The status value of such a service when listed in a Trusted List can have any of the above depicted status values as its 'current status value' (see Figure 1).

The Trusted List must contain information about the underlying supervision/accreditation scheme(s), in particular:

— Information on the supervision system applicable to any CSP_{QC};

— Information, when applicable, on the national 'voluntary accreditation' scheme applicable to any CSP_{QC};

— Information, when applicable, on the supervision system applicable to any CSP not issuing QCs;

— Information, when applicable, on the national 'voluntary accreditation' scheme applicable to any CSP not issuing QCs.

The last two sets of information are of critical importance for relying parties to assess the quality and security level of such supervision/accreditation systems applied at national level to CSPs not issuing QCs. When supervision/accreditation status information is provided in the TL with regard to services from CSPs not issuing QCs, the aforementioned sets of information shall be provided at TL level through the use of 'Scheme information URI' (clause 5.3.7 – information being provided by Member States), 'Scheme type/community/rules' (clause 5.3.9 – through the use of a text common to all Member States, and optional specific information provided by a Member State) and 'TSL policy/legal notice' (clause 5.3.11 – a text common to all Member States referring to Directive 1999/93/EC, together with the ability for each Member State to add Member State specific text/references). Additional 'qualification' information defined at the level of national supervision/accreditation systems for CSPs not issuing QCs may be provided at the service level when applicable and required (e.g. to distinguish between several quality/security levels) through the use of 'additionalServiceInformation' extension (clause 5.8.2) as part of 'Service information extension' (clause 5.5.9). Further information on the corresponding technical specifications is provided in the detailed specifications in Chapter I.

Despite the fact that separate bodies of a Member State may be in charge of the supervision and accreditation of certification services in that Member State, it is expected that only one entry shall be used for one single certification service (identified by its 'Service digital identity' as per ETSI TS 102 231 [1]) and that its supervision/accreditation status will be updated accordingly. The meaning of the above depicted statuses is described in the related clause 5.5.4 of the detailed technical specifications in Chapter I.

2.2. *TL entries aiming at facilitating the validation of QES and $AdES_{QC}$*

The most critical part of the creation of the TL is the establishment of the mandatory part of the TL, namely the 'List of services' per CSP issuing QCs, in order to correctly reflect the exact issuing situation of each such QC-issuing certification service and to ensure that the information provided in each entry is sufficient to facilitate the validation of QES and $AdES_{QC}$ (when combined with the content of the end-entity QC issued by the CSP under the certification service listed in this entry).

[1] ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information

▼C1

Insofar as there is no truly interoperable and cross-border profile for the QC, the required information might include other information than the 'Service digital identity' of a single (Root) CA, in particular information identifying the QC status of the issued certificate, and whether or not the supported signatures are created by an SSCD. The Body in a Member State that is designated to establish, edit and maintain the TL (i.e. the Scheme operator as per ETSI TS 102 231) must therefore take into account the current profile and certificate content in each issued QC, per CSP_{QC} covered by the TL.

Ideally each issued QC should include the ETSI defined QcCompliance ([1]) statement when it is claimed that it is a QC and should include the ETSI defined QcSSCD statement when it is claimed that it is supported by an SSCD to generate eSignatures, and/or that each issued QC includes one of the QCP/QCP + certificate policy Object Identifiers (OIDs) defined in ETSI TS 101 456 ([2]). The use by CSPs issuing QCs of different standards as references, the wide degree of interpretation of those standards as well as the lack of awareness of the existence and precedence of some normative technical specifications or standards has resulted in differences in the actual content of currently issued QCs (e.g. the use or not of those QcStatements defined by ETSI) and consequently are preventing the receiving parties from simply relying on the signatory's certificate (and associated chain/path) to assess, at least in a machine readable way, whether or not the certificate supporting an eSignature is claimed to be a QC and whether or not it is associated with an SSCD through which the eSignature has been created.

Completing the 'Service type identifier' (Sti), 'Service name' (Sn), and 'Service digital identity' (Sdi) ([3]) fields with information provided in the 'Service information extensions' (Sie) field allows the proposed TL common template to fully determine a specific type of qualified certificate issued by a listed CSP certification service issuing QCs and to provide information about the fact that it is supported by an SSCD or not (when such information is missing in the issued QC). A specific 'Service current status' (Scs) information is of course associated to this entry. This is depicted in Figure 2 below.

Listing a service by just providing the 'Sdi' of a (Root) CA would mean that it is ensured (by the CSP issuing QCs but also by the Supervisory/Accreditation Body in charge of the supervision/accreditation of this CSP) that any end-entity certificate issued under this (Root) CA (hierarchy) contains enough ETSI defined and machine-processable information to assess whether or not it is a QC, and whether it is supported by an SSCD. In the event, for example, that the latter assertion is not true (e.g. there is no ETSI standardised machine-processable indication in the QC about whether it is supported by an SSCD), then by listing only the 'Sdi' of that (Root) CA, it can only be assumed that QCs issued under this (Root) CA hierarchy are not supported by any SSCD. In order to consider those QCs as supported by an SSCD, the 'Sie' should be used to indicate this fact (this also indicates that it is guaranteed by the CSP issuing QCs and supervised/accredited by the Supervisory or Accreditation Body respectively).

([1]) Refer to ETSI TS 101 862 — Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.

([2]) ETSI TS 101 456 — Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

([3]) i.e., and as a minimum, an X.509 v3 certificate of the issuing QCA or of an upper CA in the certification path.

▼C1

General principles — Editing rules — CSP_{QC} entries (listed services)

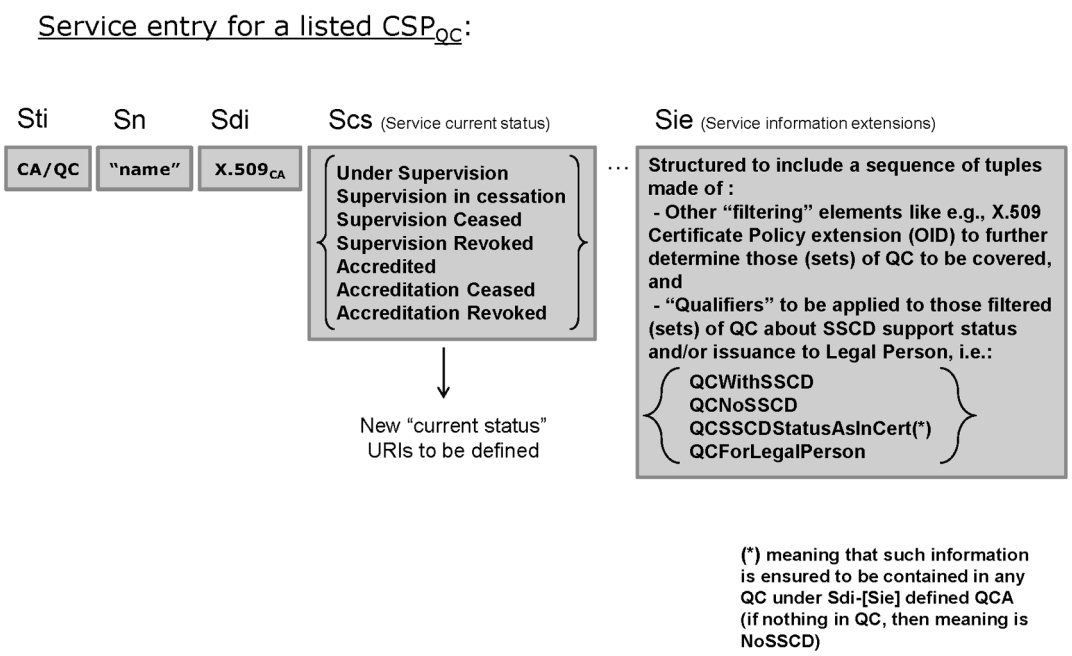


Figure 2

Service entry for a Listed CSP issuing QCs in the TL implemented in TSL format

The present TL common template technical specifications allow using a combination of five main parts of information in the service entry:

— The 'Service type identifier' (Sti), e.g. identifying a CA issuing QCs (CA/QC),

— The 'Service name' (Sn),

— The 'Service digital identity' (Sdi) information identifying a listed service, e.g. the X.509v3 certificate (as a minimum) of a CA issuing QCs,

— For CA/QC services, optional 'Service information extensions' (Sie) information that shall allow inclusion of a sequence of one or more tuples, each tuple providing:

  — Criteria to be used to further identify (filter) under the 'Sdi' identified certification service that precise service (i.e. set of qualified certificates) for which additional information is required/provided with regard to the indication of the SSCD support (and/or issuance to a Legal Person); and

  — The associated information (qualifiers) on whether this further identified service set of qualified certificates is supported by an SSCD or not or whether this associated information is part of the QC under a standardised machine-processable form, and/or information regarding the fact that such QCs are issued to Legal Persons (by default they are to be considered as issued only to Natural Persons);

▼C1

— The ‘current status’ information for this service entry providing information on:

— Whether it is a supervised or accredited service, and

— The supervision/accreditation status itself.

2.3. *Editing and usage guidelines for CSP_{QC} services entries*

The **general editing guidelines** are:

1. If it is ensured (guarantee provided by CSP_{QC} and supervised/accredited by Supervisory Body (SB)/Accreditation Body (AB)) that, for a listed service identified by a ‘Sdi’, any QC supported by an SSCD does contain the ETSI defined QcCompliance statement, and does contain the QcSSCD statement and/or QCP + Object Identifier (OID), then the use of an appropriate ‘Sdi’ is sufficient and the ‘Sie’ field can be used as an option and will not need to contain the SSCD support information.

2. If it is ensured (guarantee provided by CSP_{QC} and supervised/accredited by SB/AB) that, for a listed service identified by a ‘Sdi’, any QC not supported by an SSCD does contain either the QcCompliance statement and/or QCP OID, and it is such that it is meant to not contain the QcSSCD statement or QCP + OID, then the use of an appropriate ‘Sdi’ is sufficient and the ‘Sie’ field can be used as an option and will not need to contain the SSCD support information (meaning it is not supported by an SSCD)

3. If it is ensured (guarantee provided by CSP_{QC} and supervised/accredited by SB/AB) that, for a listed service identified by a ‘Sdi’, any QC does contain the QcCompliance statement, and some of these QCs are meant to be supported by SSCDs and some not (e.g. this may be differentiated by different CSP specific Certificate Policy OIDs or through other CSP specific information in the QC, directly or indirectly, machine-processable or not), but it contains NEITHER the QcSSCD statement NOR the ETSI QCP(+) OID, then the use of an appropriate ‘Sdi’ may not be sufficient AND the Sie field must be used to indicate explicit SSCD support information together with a potential information extension to identify the covered set of certificates. This is likely to require the inclusion of different ‘SSCD support information values’ for the same ‘Sdi’ when making use of the ‘Sie’ field.

4. If it is ensured (guarantee provided by CSP_{QC} and supervised/accredited by SB/AB) that for a listed service identified by a ‘Sdi’, any QC does not contain any of the QcCompliance statement, the QCP OID, the QcSSCD statement, or the QCP + OID but it is ensured that some of these end-entity certificates issued under this ‘Sdi’ are meant to be QCs and/or supported by SSCDs and some not (e.g. this may be differentiated by different CSP_{QC} specific Certificate Policy OIDs or through other CSP_{QC} specific information in the QC, directly or indirectly, machine-processable or not), then the use of an appropriate Sdi will not be sufficient AND the Sie field must be used to include explicit SSCD support information. This is likely to require the inclusion of different ‘SSCD support information values’ for the same ‘Sdi’ when making use of the ‘Sie’ field.

▼C1

As a general default principle, for a listed CSP in the Trusted List there must be one service entry per single X.509v3 certificate for a CA/QC type certification service, i.e. a Certification Authority (directly) issuing QCs. In some carefully envisaged circumstances and carefully managed conditions, a Member State Supervisory Body/Accreditation Body may decide to use the X.509v3 certificate of a Root or Upper level CA (i.e. a Certification Authority not directly issuing end-entity QCs but certifying a hierarchy of CAs down to CAs issuing QCs to end-entities) as the Sdi of a single entry in the list of services from a listed CSP. The consequences (advantages and disadvantages) of using such X.509v3 Root CA or Upper CA as Sdi values of TL services entries must be carefully considered and endorsed by Member States. Moreover, when using this authorized exception to the default principle, Member State must provide the necessary documentation to facilitate certification path building and verification.

In order to illustrate the general editing guidelines, the following example can be given: In the context of a CSP_{QC} using one Root CA under which several CAs are issuing QCs and non-QCs, but for which the QCs do contain only the QcCompliance statement and no indication of whether it is supported by an SSCD, listing the Root CA 'Sdi' only would mean, under the rules explained above, that any QC issued under this Root CA hierarchy is NOT supported by an SSCD. If those QCs are actually supported by an SSCD, it would be strongly recommended to make use of the QcSSCD statement in the QCs issued in the future. In the meantime (until the last QC not containing this information has expired), the TSL should make use of the Sie field and associated Qualifications extension, e.g. filtering certificates through specific CSP_{QC} defined OID(s) potentially used by the CSP_{QC} to distinguish between different types of QCs (some supported by an SSCD and some not) and including explicit 'SSCD support information' with regards to those filtered certificates through the use of 'Qualifiers'.

The **general usage guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the present Technical Specifications are as follows:

A 'CA/QC''Sti' entry (similarly a CA/QC entry further qualified as being a RootCA/QC through the use of 'Sie' additionalServiceInformation extension)

— indicates that from the 'Sdi' identified CA (similarly within the CA hierarchy starting from the 'Sdi' identified RootCA), all issued end-entity certificates are QCs **provided** that it is claimed as such in the certificate through the use of appropriate QcStatements (i.e. QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs (and this is ensured by Supervisory/Accreditation Body, see above 'general editing guidelines')

Note: if no 'Sie''Qualification information' is present or if an end-entity certificate that is claimed to be a QC is not 'further identified' through a related 'Sie' entry, then the 'machine-processable' information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate QcStatements (i.e. QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP_{QC}.

▼C1

— **and IF**‘Sie’‘Qualification’ information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this ‘Sie’‘Qualification’ entry, which is constructed on the principle of a sequence of ‘filters’ further identifying a set of certificates and providing some additional information regarding ‘SSCD support’ and/or ‘Legal person as subject’ (e.g. those certificates containing a specific OID in the Certificate Policy extension, and/or having a specific ‘Key usage’ pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.), are to be considered according to the following set of ‘qualifiers’, compensating for the lack of information in the corresponding QC, i.e.:

— to indicate the SSCD support:

  — ‘QCWithSSCD’ qualifier value meaning ‘QC supported by an SSCD’, or

  — ‘QCNoSSCD’ qualifier value meaning ‘QC not supported by an SSCD’, or

  — ‘QCSSCDStatusAsInCert’ qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the ‘Sdi’ - ‘Sie’ provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

  — ‘QCForLegalPerson’ qualifier value meaning ‘Certificate issued to a Legal Person’.

2.4. *Services supporting ‘CA/QC’ services but not part of the ‘CA/QC’‘Sdi’*

The cases where the CRLs and OCSP responses are signed by keys other than from a CA issuing QCs (‘CA/QC’) should also be covered. This may be covered by listing those services as such in the TSL implementation of the TL (i.e. with a ‘Service type identifier’ further qualified by an ‘additionalServiceInformation’ extension reflecting an OCSP or a CRL service as being part of the provision of QCs, e.g. with a service type of ‘OCSP/QC’ or ‘CRL/QC’ respectively) since these services can be considered as part of the supervised/accredited ‘qualified’ services related to the provision of QC certification services. Of course, OCSP responders or CRL Issuers whose certificates are signed by CAs under the hierarchy of a listed CA/QC service are to be considered as ‘valid’ and in accordance with the status value of the listed CA/QC service.

A similar provision can apply to certification services issuing non-qualified certificates (of a ‘CA/PKC’ service type) using the default ETSI TS 102 231 OCSP and CRL service types.

Note that the TSL implementation of the TL MUST include revocation services when related information is not present in the AIA field of end certificates, or when not signed by a CA that is one of the listed CAs.

2.5. *Moving towards interoperable QC profile*

As a general rule, it must be tried to simplify (reduce) as far as possible the number of entries of services (different ‘Sdi’’s). This must be balanced however with the correct identification of those services that are related to the issuing of QCs and the provision of the trusted information on whether or not those QCs are supported by an SSCD when this information is missing from the issued QC.

▼C1

Ideally the use of the 'Sie' field and 'Qualification' extension should be (strictly) restricted to those specific cases to be solved that way, as QCs should contain enough information with regard to the claimed qualified status and the claimed support or not by an SSCD.

Member States should, as much as possible, enforce the adoption and use of interoperable QC profiles.

3. **Structure of the Common Template for the Trusted List**

The proposed Common Template for a Member State Trusted List will be structured into the following categories of information:

1. Information on the Trusted List and its issuing scheme;

2. A sequence of fields holding unambiguous identification information about every supervised/accredited CSP under the scheme (this sequence is optional, i.e. when not used, the list will be deemed to be empty meaning that no CSP is either supervised or accredited in the associated Member State in the context of the Trusted List scope);

3. For each listed CSP, a sequence of fields holding unambiguous identification of a supervised/accredited certification service provided by the CSP (this sequence must have a minimum of one entry);

4. For each listed supervised/accredited certification service, identification of the current status of the service and the history of this status.

In the context of a CSP issuing QCs, the unambiguous identification of a supervised/accredited certification service to be listed must take into consideration those situations where not enough information is available in the qualified certificate about its 'qualified' status, its potential support by an SSCD and especially in order to cope with the additional fact that most of the (commercial) CSPs are using one single issuing Qualified CA to issue several types of end-entity certificates, both qualified and non-qualified.

The number of entries in the list per recognised CSP might be reduced where one or several Upper CA services exist, e.g. in the context of a commercial hierarchy of CAs from a Root CA down to issuing CAs. However even in those cases, the principle of ensuring the unambiguous link between a CSP_{QC} certification service and the set of certificates meant to be identified as QCs has to be maintained and ensured.

1. *Information on the Trusted List and its issuing scheme*

The following information will be part of this category:

— A Trusted List tag facilitating the identification of the Trusted List during electronic searches and also to confirm its purposes when in human-readable form,

— A Trusted List format and format version identifier,

— A Trusted List sequence (or release) number,

— A Trusted List **type information** (e.g. for identification of the fact that this Trusted List is providing information on the supervision/accreditation status of certification services from CSPs supervised/accredited by the referenced Member State for compliance with the provisions laid down in Directive 1999/93/EC);

▼C1

— A Trusted List owner information (e.g. name, address, contact information, etc. of the Member State Body in charge of establishing, publishing securely and maintaining the Trusted List),

— Information about the underlying supervision/accreditation scheme(s) to which the Trusted List is associated, including but not limited to:

  — the country in which it applies,

  — information on or reference to the location where information on the scheme(s) can be found (scheme model, rules, criteria, applicable community, type, etc.),

  — period of retention of (historical) information;

— Trusted List policy and/or legal notice, liabilities, responsibilities,

— Trusted List issue date and time and next foreseen update,

2. *Unambiguous identification information about every CSP recognised by the scheme*

This set of information will include at least the following:

— The CSP organisation name as used in formal legal registrations (this may include the CSP organisation UID following Member State practices),

— The CSP address and contact information,

— Additional information on the CSP either included directly or by reference to a location from where such information can be downloaded,

3. *For each listed CSP, a sequence of fields holding unambiguous identification of a certification service provided by the CSP and supervised/ accredited in the context of Directive 1999/93/EC*

This set of information will include at least the following for each certification service from a listed CSP:

— An identifier of the type of certification service (e.g. identifier indicating that the supervised/accredited certification service from the CSP is a Certification Authority issuing QCs),

— (Trade) name of this certification service,

— An unambiguous unique identifier of the certification service,

— Additional information on the certification service (e.g. directly included or included by reference to a location from which information can be downloaded, access information regarding the service),

— For CA/QC services, an optional sequence of tuples of information, each tuple providing,

  (i) Criteria to be used to further identify (filter) within the 'Sdi' identified certification service that precise service (i.e. set of qualified certificates) for which additional information is required/provided with regards to the indication of the SSCD support (and/or issuance to Legal Person); and

  (ii) The associated 'qualifiers' providing information whether the set of qualified certificates from this further identified service is supported by an SSCD or not, and/or information about whether such QCs are issued to Legal Person (by default they are to be considered as issued to Natural Persons).

▼C1

4. *For each listed certification service, the identification of the current status of the service and the history of this status*

This set of information will include at least the following:

— An identifier of the Current Status;

— The Current Status starting date and time;

— Historical information about this status.

4. **Definitions and abbreviations**

For the purposes of the present document, the following definitions and acronyms apply:

Term	Acronym	Definition
Certification Service Provider	CSP	As defined in Article 2(11) of Directive 1999/93/EC
Certification Authority	CA	A CA is a CSP and can use several technical CAs' private signing keys, each having an associated certificate, in order to issue end-entity certificates. A CA is an authority trusted by one or more users to create and assign certificates. Optionally the Certification Authority may create the users' keys [ETSI TS 102 042]. The CA is deemed to be identified through the identification information present in the Issuer field of the CA certificate related to (certifying) the public key associated with the CA's private signing key and which, effectively, is used by the CA to issue entity certificates. A CA may have several signing keys. Every CA signing key is uniquely identified by a unique identifier as part of the Authority Key Identifier field in the CA's certificate.
Certification Authority issuing Qualified Certificates	CA/QC	A CA who meets the requirements laid down in Annex II of Directive 1999/93/EC and issues qualified certificates meeting the requirements laid down in Annex I of Directive 1999/93/EC.
Certificate	Certificate	As defined in Article 2.9 of Directive 1999/93/EC
Qualified Certificate	QC	As defined in Article 2(10) of Directive 1999/93/EC
Signatory	Signatory	As defined in Article 2(3) of Directive 1999/93/EC
Supervision	Super-vision	Supervision is used in the meaning of Directive 1999/93/EC (Art. 3,3). The Directive requires Member States to establish an appropriate system allowing the supervision of CSPs which are established on their territory and issue qualified certificates to the public, ensuring the supervision of compliance with the provisions laid down in the Directive.
Voluntary Accredi-tation	Accredi-tation	As defined in article 2(13) of Directive 1999/93/EC
Trusted List	TL	Designates the list indicating the supervision/accreditation status of certification services from Certification Services Providers who are supervised/accredited by the referenced Member State for compliance with the provisions laid down in Directive 1999/93/EC.

▼C1

Term	Acronym	Definition
Trust-service Status List	TSL	Form of a signed list used as the basis for presentation of trust service status information according to the specifications laid down in the ETSI TS 102 231.
Trust Service		Service which enhances trust and confidence in electronic transactions (typically but not necessarily using cryptographic techniques or involving confidential material) (ETSI TS 102 231).
Trust Service Provider	TSP	Body operating one or more (electronic) Trust Services (This term is used with a broader application than CSP).
Trust Service Token	TrST	A physical or binary (logical) object generated or issued as a result of the use of a Trust Service. Examples of binary TrSTs are certificates, CRLs, Time Stamp Tokens and OCSP responses.
Qualified Electronic Signature	QES	An AdES supported by a QC and which is created by an SSCD as defined in Article 2 of Directive 1999/93/EC.
Advanced Electronic Signature	AdES	As defined in Article 2(2) of Directive 1999/93/EC.
Advanced Electronic Signature supported by a Qualified Certificate	$AdES_{QC}$	Means an Electronic Signature that meets the requirements of an AdES and is supported by a QC as defined in Article 2 of Directive 1999/93/EC.
Secure Signature Creation Device	SSCD	As defined in Article 2(6) of Directive 1999/93/EC.

CHAPTER I

DETAILED SPECIFICATIONS FOR THE COMMON TEMPLATE FOR THE 'TRUSTED LIST OF SUPERVISED/ACCREDITED CERTIFICATION SERVICE PROVIDERS'

Within the following part of the document the key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' are to be interpreted as described in RFC 2119 ([1]).

►**M1** The present specifications are relying on the specifications and requirements stated in ETSI TS 102 231 v.3.1.2. When no specific requirement is stated in the present specifications, requirements from ETSI TS 102 231 v.3.1.2 SHALL apply entirely. ◄ When specific requirements are stated in the present specifications, they SHALL prevail over the corresponding requirements from ETSI TS 102 231 while being completed by format specifications specified in ETSI TS 102 231. In case of discrepancies between the present specifications and specifications from ETSI TS 102 231, the present specifications SHALL be the normative ones.

([1]) IETF RFC 2119: 'Key words for use in RFCs to indicate Requirements Levels'.

▼C1

Language support SHALL be implemented and provided at least in English (EN) and potentially additionally in one or more national languages.

Date-time indication SHALL be compliant with clause 5.1.4 of ETSI TS 102 231.

Use of URIs SHALL be compliant with clause 5.1.5 of ETSI TS 102 231.

Information on the Trusted List Issuing Scheme

Tag

TSL tag (clause 5.2.1)

This field is REQUIRED and SHALL comply with clause 5.2.1 of ETSI TS 102 231.

▼M1

———————

▼C1

Scheme Information

TSL version identifier (clause 5.3.1)

This field is REQUIRED and SHALL be set to '3' (integer).

TSL sequence number (clause 5.3.2)

▼M1

This field is REQUIRED. It SHALL specify the sequence number of the TSL. Starting from '1' at the first release of the TSL, this integer value SHALL be incremented at each subsequent release of the TSL. It SHALL NOT be recycled to '1' when the 'TSL version identifier' above is incremented.

▼C1

TSL type (clause 5.3.3)

▼M1

This field is REQUIRED specifying the type of TSL. It SHALL be set to http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic).

▼C1

Note: In order to comply with ETSI TS 102 231, clause 5.3.3, and to indicate the specific type of TSL while referring to the existence of the present specifications ruling the establishment of the TSL implementation of the Member States' Trusted List ([1]) and permitting a parser to determine which form of any following fields ([2]) to expect, where those fields have specific (or alternative) meanings according to the type of the TSL represented (in this case being a Trusted List of a Member State), the above specific URI SHALL be registered and described as follows:

([1]) i.e., the 'Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC' (in short the 'Trusted List').

([2]) Meaning the fields specified by ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information and 'profiled' by the present specifications to specify the establishment of the Member States' Trusted List.

▼**M1**

URI: (Generic) http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic

▼**C1**

Description: A TSL implementation of a supervision/accreditation status list of certification services from certification service providers which are supervised/accredited by the referenced Member State owning the TSL implementation for compliance with the relevant provisions laid down in Directive 1999/93/EC, through a process of direct oversight (whether voluntary or regulatory).

Scheme operator name (clause 5.3.4)

This field is REQUIRED. It SHALL specify the name of the Member State's Body in charge of establishing, publishing and maintaining the National Trusted List. It SHALL specify the formal name under which the associated legal entity or mandated entity (e.g. for governmental administrative agencies) associated with this Body operates. It MUST be the name used in formal legal registration or authorisation and to which any formal communication should be addressed. It SHALL be a Sequence of multilingual character strings and SHALL be implemented with English (EN) as the mandatory language and with potentially one or more national language(s).

Note: A country MAY have separate Supervisory and Accreditation Bodies and even additional bodies for whatever operational related activities. ►**M1** It is up to each Member State to designate the Scheme operator of the TSL implementation of the Member State TL. ◄ It is expected that the Supervisory Body, the Accreditation Body and the Scheme Operator (when they appear to be separate bodies) will each of them have their own responsibility and liability.

Any situation in which several bodies are responsible for supervision, accreditation or operational aspects SHALL be consistently reflected and identified as such in the Scheme information as part of the TL, including in the scheme-specific information indicated by the 'Scheme information URI' (clause 5.3.7).

▼**M1**

The named Scheme Operator (clause 5.3.4) is the entity who will sign the TSL.

▼**C1**

Scheme operator address (clause 5.3.5)

This field is REQUIRED. It SHALL specify the address of the legal entity or mandated organization identified in the 'Scheme operator name' field (clause 5.3.4) for both postal and electronic communications. It SHALL include both 'PostalAddress' (i.e. street address, locality, [state or province], [postal code] and ISO 3166-1 alpha-2 country code) as compliant with clause 5.3.5.1; and 'ElectronicAddress' (i.e. e-mail and/or website URI) as compliant with clause 5.3.5.2.

Scheme name (clause 5.3.6)

This field is REQUIRED specifying the name under which the scheme operates. It SHALL be a sequence of multilingual character strings (with EN as the mandatory language, and with potentially one or more national languages) defined as follows:

▼C1

— The EN version SHALL be a character string structured as follows:

CC:EN_name_value

where

— ‘CC’ = the ISO 3166-1 alpha-2 Country Code used in the ‘Scheme territory field’ (clause 5.3.10);

— ‘:’ = is used as the separator;

▼M1

— ‘EN_name_value’ = Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State’s laws;

▼C1

— Any Member State’s national language version SHALL be a character string structured as follows:

CC:name_value

where

— ‘CC’ = the ISO 3166-1 alpha-2 Country Code used in the ‘Scheme territory field’ (clause 5.3.10);

— ‘:’ = is used as the separator;

— ‘name_value’ = National language official translation of the above EN_name_value.

The scheme name is required to uniquely identify, by name, the scheme referred to by the Scheme information URI, and also to ensure that in case a scheme operator operates more than one scheme, there is a distinct name given to each of them.

Member States and Scheme operators SHALL make sure that when a Member State or a Scheme Operator operates more than one scheme, there is a distinct name given to each of them.

Scheme information URI (clause 5.3.7)

This field is REQUIRED and SHALL specify the URI(s) where users (relying parties) can obtain scheme-specific information (with EN as the mandatory language and with potentially one or more national languages). This SHALL be a sequence of multilingual pointers (with EN as the mandatory language, and with potentially one or more national languages). The referenced URI(s) MUST provide a path to information describing ‘appropriate information about the scheme’.

The appropriate information about the scheme SHALL include as a minimum:

— General introductory information that would be common to all Member States with regard to the scope and context of the Trusted List, and the underlying supervision/accreditation scheme(s). The common text to be used is as follows:

▼C1

‘The present list is the TSL implementation of [*name of the relevant Member State*] “Trusted List of supervised/accredited Certification Service Providers” providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3,3, 3.2 and Art. 7.1(a)), including information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable “supervision” system (respectively “voluntary accreditation” system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3,3, Art. 8,1, Art. 11 (respectively, Art. 2,13, Art. 3,2, Art 7.1(a), Art. 8,1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.’

— Specific information on the underlying supervision/accreditation scheme(s), in particular ([1]):

— Information on the supervision system applicable to any CSP_{QC};

([1]) The last two sets of information are of critical importance for relying parties to assess the quality and security level of such supervision/accreditation systems. Those sets of information shall be provided at TL level through the use of the present ‘Scheme information URI’ (clause 5.3.7 — information being provided by Member State), ‘Scheme type/community/rules’ (clause 5.3.9 — through the use of a text common to all Member States) and ‘TSL policy/legal notice’ (clause 5.3.11 — a text common to all Member States referring to Directive 1999/93/EC, together with the ability for each Member State to add Member State specific text/references). Additional information on national supervision/accreditation systems for CSPs not issuing QCs may be provided at service level when applicable and required (e.g. to distinguish between several quality/security levels) through the use of ‘Scheme service definition URI’ (clause 5.5.6).

▼C1

— Information, when applicable, on the national voluntary accreditation scheme applicable to any CSP_{QC};

— Information, when applicable, on the supervision system applicable to any CSP not issuing QCs;

— Information, when applicable, on the national voluntary accreditation scheme applicable to any CSP not issuing QCs;

— This specific information SHALL include, at least, for each underlying scheme listed above:

— General description;

— Information about the process followed by the Supervisory/Accreditation Body to supervise/accredit CSPs and by the CSPs for being supervised/accredited;

— Information about the criteria against which CSPs are supervised/accredited.

— Specific information, when applicable, on the specific qualifications some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive on the basis of their compliance with the provisions and requirements laid down at national level including the meaning of such a qualification and the associated national provisions and requirements.

Additional Member State specific information about the scheme MAY additionally be provided on a voluntary basis. This SHALL include:

— Information about the criteria and rules used to select supervisors/auditors and defining how CSPs are supervised (controlled)/accredited (audited) by them;

— Other contact and general information that applies to the scheme operation.

Status determination approach (clause 5.3.8)

This field is REQUIRED and SHALL specify the identifier of the status determination approach. The following specific URI SHALL be used, as registered and described as follows:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/appropriate

Description: Services listed have their status determined by or on behalf of the Scheme Operator under an appropriate system for a referenced Member State that allows for ‘supervision’ (and, when applicable, for ‘voluntary accreditation’) of certification service providers who are established on its territory (or established in a third country in the case of ‘voluntary accreditation’) and issue qualified certificates to the public according to Art. 3,3 (respectively Art. 3,2 or Art. 7.1(a)) of the Directive 1999/93/EC, and, when applicable, that allows for the ‘supervision’/‘voluntary accreditation’ of certification service providers not issuing qualified certificates, according to a nationally defined and established recognised ‘approval scheme(s)’ implemented on a national basis for the supervision of compliance of services from CSPs not issuing QCs with the provisions laid down in Directive 1999/93/EC and potentially extended by national provisions with regard to the provision of such certification services.

▼C1

Scheme type/community/rules (clause 5.3.9)

This field is REQUIRED and SHALL contain at least the following registered URIs:

— A URI common to all Member States' Trusted Lists pointing towards a descriptive text that SHALL be applicable to all TLs:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

— By which participation is denoted of the Member State's scheme (identified via the TSL type (clause 5.3,3) and Scheme name (clause 5.3.6)) in a scheme of schemes (i.e. a TSL listing pointers to all Member States publishing and maintaining a TL in the form of a TSL);

— Where users can obtain policy/rules against which services included in the list SHALL be assessed and from which the type of the TSL (see clause 5.3.3) can be determined;

— Where users can obtain description about how to use and interpret the content of the TSL implementation of the Trusted List. These usage rules SHALL be common to all Member States' Trusted Lists whatever the type of listed service and whatever the supervision/accreditation system(s) is (are).

Descriptive text:

'Participation in a scheme

Each Member State must create a "Trusted List of supervised/accredited Certification Service Providers" providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The present TSL implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's TSL implementation of their Trusted List, compiled by the European Commission.

Policy/rules for the assessment of the listed services

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3,2 and Art. 7.1(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

▼C1

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable "supervision" system (respectively "voluntary accreditation" system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3,3, Art. 8,1, Art. 11 (respectively, Art.2.13, Art. 3,2, Art 7.1(a), Art. 8,1, Art. 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a "voluntary accreditation" system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined "recognised approval scheme" implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Art. 2,11 of the Directive). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific "qualification" on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a "qualification" is likely to be limited solely to the national level.

Interpretation of the TSL implementation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision 2009/767/EC are as follows:

A "CA/QC""Service type identifier" (Sti) entry (similarly a CA/QC entry further qualified as being a "RootCA/QC" through the use of "Service information extension" (Sie) additionalServiceInformation extension)

— indicates that from the "Service digital identifier" (Sdi) identified CA (similarly within the CA hierarchy starting from the "Sdi" identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) **provided** that it is claimed as such in the certificate through the use of appropriate ETSI TS 101 862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101 456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C1

Note: if no “Sie”“Qualification” information is present or if an end-entity certificate that is claimed to be a QC is not “further identified” through a related Sie entry, then the “machine-processable” information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— **and IF**“Sie”“Qualification” information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this Sie Qualification entry, which is constructed on the principle of a sequence of “filters” further identifying a set of certificates, must be considered according to the associated qualifiers providing some additional information regarding SSCD support and/or “Legal person as subject” (e.g. those certificates containing a specific OID in the Certificate Policy extension, and/or having a specific “Key usage” pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). Those qualifiers are part of the following set of “qualifiers” used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

— to indicate the nature of the SSCD support:

— “QCWithSSCD” qualifier value meaning “QC supported by an SSCD”, or

— “QCNoSSCD” qualifier value meaning “QC not supported by an SSCD”, or

— “QCSSCDStatusAsInCert” qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the “Sdi”-“Sie” provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

— “QCForLegalPerson” qualifier value meaning “Certificate issued to a Legal Person”

The general interpretation rule for any other “Sti” type entry is that the listed service named according to the “Sn” field value and uniquely identified by the “Sdi” field value has a current supervision/accreditation status according to the “Scs” field value as from the date indicated in the “Current status starting date and time”. Specific interpretation rules for any additional information with regard to a listed service (e.g. “Service information extensions” field) may be found, when applicable, in the Member State specific URI as part of the present “Scheme type/community/rules” field.

Please refer to the Technical specifications for a Common Template for the “Trusted List of supervised/accredited Certification Service Providers” in the Annex of Commission Decision 2009/767/EC for further details on the fields, description and meaning for the TSL implementation of the Member States' Trusted Lists.’

▼C1

— A URI specific to each Member State's Trusted List pointing towards a descriptive text that SHALL be applicable to this Member State TL:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC

where CC = the ISO 3166-1 alpha-2 Country Code used in the 'Scheme territory' field (clause 5.3.10)

— Where users can obtain the referenced Member State's specific policy/rules against which services included in the list SHALL be assessed in compliance with the Member State's appropriate supervision system and voluntary accreditation schemes.

— Where users can obtain a referenced Member State's specific description about how to use and interpret the content of the TSL implementation of the Trusted List with regard to the certification services not related to the issuing of QCs. This may be used to indicate a potential granularity in the national supervision/accreditation systems related to CSPs not issuing QCs and how the 'Scheme service definition URI' (clause 5.5.6) and the 'Service information extension' field are used for this purpose.

Member States MAY define additional URIs from the above Member State specific URI (i.e. URIs defined from this hierarchical specific URI).

Scheme territory (clause 5.3.10)

In the context of the present specifications, this field is REQUIRED and SHALL specify the country in which the scheme is established (ISO 3166-1 alpha-2 country code).

TSL policy/legal notice (clause 5.3.11)

In the context of the present specifications, this field is REQUIRED and SHALL specify the scheme's policy or provide a notice concerning the legal status of the scheme or legal requirements met by the scheme for the jurisdiction in which the scheme is established and/or any constraints and conditions under which the TL is maintained and published.

This SHALL be a multilingual character string (plain text) made of two parts:

— A first mandatory part, common to all Member States' TLs (with EN as the mandatory language, and with potentially one or more national languages), indicating that the applicable legal framework is Directive 1999/93/EC and its corresponding implementation in the laws of the Member State indicated in the 'Scheme Territory' field.

English version of the common text:

'The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.'

▼C1

Text in a Member State's national language(s): [official translation(s) of the above English text].

— A second optional part, specific to each TL (with EN as the mandatory language, and with potentially one or more national languages), indicating references to specific applicable national legal frameworks (e.g. in particular when related to national supervision/accreditation schemes for CSPs not issuing QCs).

Historical information period (clause 5.3.12)

This field is REQUIRED and SHALL specify the duration (integer) over which historical information in the TSL is provided. This integer value is to be provided in number of days and in the context of the present specifications it SHALL be greater or equal to 3 653 (i.e. meaning that the TSL implementation of Member States' TL MUST contain historical information for a minimum of ten years). Greater values should take due account of the legal requirements for data retention in the Member State indicated in the 'Scheme Territory' (clause 5.3.10).

Pointers to other TSLs (clause 5.3.13)

In the context of the present specifications, this field is REQUIRED and SHALL include, when this is available, the pointer to an ETSI TS 102 231 compliant form of the EC compiled list of links (pointers) towards all TSL implementations of Trusted Lists from the Member States. Specifications from ETSI TS 102 231, clause 5.3.13 shall apply while mandating the use of the optional digital identity, representing the issuer of the TSL pointed to, formatted as specified in clause 5.5.3.

Note: While waiting for the ETSI TS 102 231 compliant implementation of the EC compiled list of links towards Members State's TSL implementation of their TLs, this field SHALL NOT be used.

List issue date and time (clause 5.3.14)

This field is REQUIRED and SHALL specify the date and time (UTC expressed as Zulu) on which the TSL was issued using Date-time value as specified in ETSI TS 102 231, clause 5.1.4.

Next update (clause 5.3.15)

This field is REQUIRED and SHALL specify the latest date and time (UTC expressed as Zulu) by which the next TSL will be issued or be null to indicate a closed TSL (using Date-time value as specified in ETSI TS 102 231, clause 5.1.4).

In the event of no interim status changes to any TSP or service covered by the scheme, the TSL MUST be re-issued by the time of expiration of the last TSL issued.

In the context of the present specifications, the difference between the 'Next update' date and time and the 'List issue date and time' SHALL NOT exceed **six (6)** months.

▼C1

Distribution points (clause 5.3.16)

This field is OPTIONAL. If used, it SHALL specify locations where the current TSL implementation of the TL is published and where updates to the current TSL can be found. If multiple distribution points are specified, they all MUST provide identical copies of the current TSL or its updated version. When used, this field is formatted as non-empty sequence of strings, each of them compliant with RFC 3986 ([1]).

Scheme extensions (clause 5.3.17)

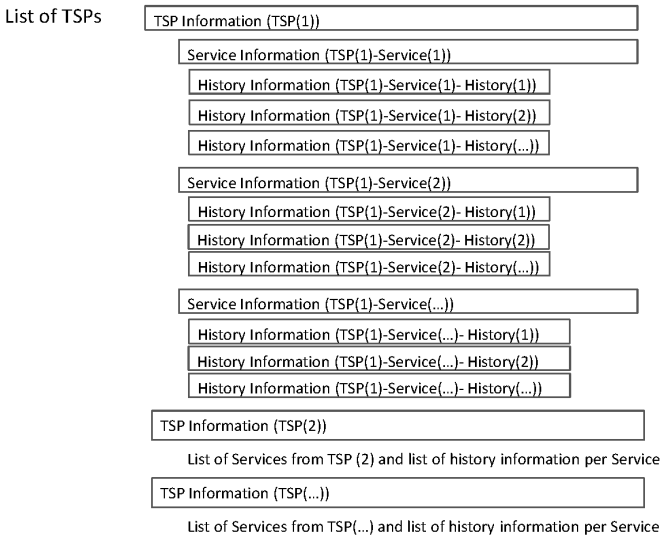
This field is OPTIONAL and is not used in the context of the present specification.

List of Trust Service Providers

This field is OPTIONAL.

In the case where no CSPs are or were supervised/accredited in the context of the scheme in a Member State, this field SHALL be absent. It is agreed, however, that even when a Member State has no CSP either supervised or accredited by the scheme, Member States SHALL implement a TSL with this field absent. The absence of any CSP in the list SHALL mean that there are no CSPs that are supervised/accredited in the country specified in the 'Scheme Territory'.

In the case one or more CSP services are or were supervised/accredited by the scheme, then the field SHALL contain a sequence identifying each CSP providing one or more of those supervised/accredited services, with details on the supervised/accredited status and status history of each of the CSP's services (TSP = CSP in the Figure below).



([1]) IETF RFC 3986: 'Uniform Resource Identifiers (URI): Generic syntax'.

▼C1

The list of TSPs is organised as depicted in the above Figure. For each TSP, there is a sequence of fields holding information on the TSP (TSP Information), followed by a list of Services. For each of such listed Services, there is a sequence of fields holding information on the Service (Service Information), and a sequence of fields on the approval status history of the Service (Service approval history).

TSP Information

TSP(1)

TSP name (clause 5.4.1)

This field is REQUIRED and SHALL specify the name of the **legal entity** responsible for the CSP's services that are or were supervised or accredited under the scheme. This is a sequence of multilingual character strings (with EN as the mandatory language and with potentially one or more national languages). This name MUST be the name which is used in formal legal registrations and to which any formal communication would be addressed.

TSP trade name (clause 5.4.2)

This field is OPTIONAL and, if present, SHALL specify an alternative name under which the CSP identifies itself in the specific context of the provision of those of its services which are to be found in this TSL under its 'TSP name' (clause 5.4.1) entry.

Note: Where a single CSP legal entity is providing services under different trade names or under different specific contexts, there might be as many CSP entries as such specific contexts (e.g. Name/Trade Name entries). An alternative is to list each and every CSP (legal entity) only once and provide Service specific context information. This is up to the Member State Scheme Operator to discuss and agree with the CSP the most suitable approach.

TSP address (clause 5.4.3)

This field is REQUIRED and SHALL specify the address of the legal entity or mandated organization identified in the 'TSP name' field (clause 5.4.1) for both postal and electronic communications. It SHALL include both 'PostalAddress' (i.e. street address, locality, [state or province], [postal code] and ISO 3166-1 alpha-2 country code) as compliant with clause 5.3.5.1; and 'ElectronicAddress' (i.e. e-mail and/or website URI) as compliant with clause 5.3.5.2.

TSP information URI (clause 5.4.4)

This field is REQUIRED and SHALL specify the URI(s) where users (e.g. relying parties) can obtain CSP specific information. This SHALL be a sequence of multilingual pointers (with EN as the mandatory language, and with potentially one or more national languages). The referenced URI(s) MUST provide a path to information describing the general terms and conditions of the CSP, its practices, legal issues, its customer care policies and other generic information which applies to all of its services listed under its CSP entry in the TSL.

Note: Where a single CSP legal entity is providing services under different trade names or under different specific contexts, and this has been reflected in as many TSP entries as such specific contexts, this field SHALL specify information related to the specific set of services listed under a particular TSP/TradeName entry.

▼C1

TSP information extensions (clause 5.4.5)

This field is OPTIONAL and, if present, MAY be used by the scheme operator, in compliance with ETSI TS 102 231 specifications (clause 5.4.5), to provide specific information, to be interpreted according to the rules of the specific scheme.

List of Services

This field is REQUIRED and SHALL contain a sequence identifying each of the CSP's recognised services and the approval status (and history of that status) of that service. At least one service must be listed (even if the information held is entirely historical).

As the retention of historical information about listed services is REQUIRED under the present specifications, that historical information MUST be retained even if the service's present status would not normally require it to be listed (e.g. the service is withdrawn). Thus a CSP MUST be included even when its only listed service is in such a state, so as to preserve the history.

Service Information

TSP(1) Service(1)

Service type identifier (clause 5.5.1)

▼M1

This field is REQUIRED and SHALL specify the identifier of the service type according to the type of the present TSL specifications (i.e. '/eSigDir-1999-93-EC-TrustedList/TSLType/generic').

▼C1

When the listed service is related to the issuing of Qualified Certificates, the quoted URI SHALL be http://uri.etsi.org/TrstSvc/Svctype/CA/QC (a Certification Authority issuing Qualified Certificates).

When the listed service is related to the issuing of Trust Service Tokens not being QCs and not supporting the issuance of QCs, the quoted URI SHALL be one of the URIs defined in ETSI 102 231 and listed in its clause D.2, pertaining to this field. This SHALL be applied even for those Trust Service Tokens that are supervised/accredited to meet some specific qualifications according to Member States' national laws (e.g. so-called Qualified Time Stamp Token in DE or HU), the quoted URI SHALL be one of the URIs defined in ETSI 102 231 and listed in its clause D.2, pertaining to this field (e.g. TSA for nationally defined Qualified Time Stamp Tokens). When applicable such specific national qualification of the Trust Service Tokens MAY be provided in the service entry, and the additionalServiceInformation extension (clause 5,8.2) in clause 5.5.9 (Service information extension) SHALL be used for this purpose.

▼C1

As a general default principle, there SHALL be one entry per single X.509v3 certificate (e.g. for a CA/QC type certification service) under the listed certification services from a listed CSP in the Trusted List (e.g. a Certification Authority (directly) issuing QCs). In some carefully envisaged circumstances and carefully managed and endorsed conditions, a Member State's Supervisory Body/Accreditation Body MAY decide to use the X.509v3 certificate of a Root or Upper level CA (e.g. a Certification Authority not directly issuing end-entity QCs but certifying a hierarchy of CAs down to CAs issuing QCs to end-entities) as the 'Sdi' of a single entry in the list of services from a listed CSP. The consequences (advantages and disadvantages) of using such X.509v3 Root CA or Upper CA certificate as 'Sdi' value of TL services entries must be carefully considered and endorsed by Member States [1]. In addition, when using such an authorized exception to the default principle, Member States MUST provide the necessary documentation to facilitate the certification path building and verification.

Note: TSPs like OCSP responders and CRL Issuers that are part of CSP_{QC} certification services and subject to the use of separate key pairs to respectively sign OCSP responses and CRLs MAY be listed as well in the present TSL template by using the following combination of URIs:

— 'Service type identifier' (clause 5.5.1) value:

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

combined with the following 'Service information extension' (clause 5.5.9) additionalServiceInformation extension (clause 5.8.2) value:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Description: a certificate status provider operating an OCSP-server as part of a service from a CSP issuing Qualified Certificates,

— 'Service type identifier' (clause 5.5.1) value:

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

combined with the following 'Service information extension' (clause 5.5.9) additionalServiceInformation extension (clause 5.8.2) value:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Description: a certificate status provider operating a CRL as part of a service from a CSP issuing Qualified Certificates,

— 'Service type identifier' (clause 5.5.1) value:

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

[1] Using a RootCA X.509v3 certificate as 'Sdi' value for a listed service, will force the Scheme Operator to consider the whole set of certification services under such a Root CA as a whole with regards to the 'supervision/accreditation status'. E.g. any status change required from one single CA under the listed root hierarchy, will force the whole hierarchy to take-on that status change.

▼C1

combined with the following ‘Service information extension’ (clause 5.5.9) additionalServiceInformation extension (clause 5.8.2) value:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Description: a Root Certification Authority from which a certification path can be established down to a Certification Authority issuing Qualified Certificates,

— ‘Service type identifier’ (clause 5.5.1) value:

http://uri.etsi.org/TrstSvc/Svctype/TSA

combined with the following ‘Service information extension’ (clause 5.5.9) additionalServiceInformation extension (clause 5.8.2) value:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Description: a time stamping service as part of a service from a certification service provider issuing Qualified Certificates that issue TST that can be used in the qualified signature verification process to ascertain and extend the signature validity when the QC is revoked or expired.

Service name (clause 5.5.2)

This field is REQUIRED and SHALL specify the name under which the CSP identified in ‘TSP name’ (clause 5.4.1) provides the service identified in ‘Service type identifier’ (clause 5.5.1). This SHALL be a sequence of multilingual character strings (with EN as the mandatory language, and with potentially one or more national languages).

Service digital identity (clause 5.5.3)

This field is REQUIRED and SHALL specify at least one representation of a digital identifier unique to the service whose type is specified in ‘Service type identifier’ (clause 5.5.1) by which the service can be unambiguously identified.

In the present specifications, the digital identifier used in this field SHALL be the relevant X.509v3 Certificate being a representation of the public key(s) that the CSP uses for providing the service whose type is specified by the ‘Service type identifier’ (clause 5.5.1) (i.e. the key used by a RootCA/QC, the key used for signing certificates [1], or alternatively issuing Time Stamp Tokens, or signing CRLs, or signing OCSP responses). This related X.509v3 Certificate SHALL be used as the minimum required digital identifier (being the representation of the public key(s) the CSP uses for providing the listed service). Additional identifiers MAY be used as follows but they all MUST refer to the same identity (i.e. the related X.509v3 certificate):

[1] This can be the certificate of a CA issuing end-entity certificates (e.g. CA/PKC, CA/QC) **or** the certificate of a trusted root CA from which a path can be found down to end-entity qualified certificates. Depending on whether or not this information and the information to be found in every end-entity certificate issued under this trusted root can be used to unambiguously determine the appropriate characteristics of any qualified certificate, this information (Service digital identity) may need to be completed by ‘Service information extensions’ data (see clause 5.5.9).

▼C1

(a) The distinguished name (DN) of the certificate which can be used to verify electronic signatures of the CSP service specified in 'Service type identifier' (clause 5.5.1);

(b) The related public key identifier (i.e. X.509v3 SubjectKeyIdentifier or SKI value);

(c) The related public key.

As a general default principle, the digital identifier (i.e. the related X.509v3 certificate) SHALL NOT be present more than once in the Trusted List, i.e. there SHALL be one entry per single X.509v3 certificate for a certification service under the listed certification services from a listed CSP in the Trusted List. Conversely, one single X.509v3 certificate SHALL be used in a single service entry as the 'Sdi' value.

Note(1): The sole case for which the above general default principle may not be applied is the situation where a single X.509v3 certificate is used when issuing different types of Trust Services' Tokens for which different supervision/accreditation schemes apply, for example a single X.509v3 certificate is used by a CSP on the one hand when issuing QCs under an appropriate supervision system and on the other hand when issuing non-qualified certificates under a different supervision/accreditation status. In this case and example, two entries with different 'Sti' values (e.g. respectively CA/QC and CA/PKC in the given example) and with the same 'Sdi' value (the related X.509v3 certificate) would be used.

Implementations are ASN.1 or XML dependent and SHALL comply with ETSI TS 102 231 specifications (for ASN.1 see Annex A of ETSI TS 102 231, and for XML see Annex B of ETSI TS 102 231).

Note(2): When additional 'qualification' information needs to be provided with regard to the identified service entry, then, when appropriate, the Scheme Operator SHALL consider the use of the 'additionalServiceInformation' extension (clause 5.8.2) of the 'Service information extension' field (clause 5.5.9) according to the purpose of providing such additional 'qualification' information. Additionally, the Scheme operator can optionally use clause 5.5.6 (Scheme service definition URI).

Service current status (clause 5.5.4)

This field is REQUIRED and SHALL specify the identifier of the status of the service through one of the following URIs:

— **Under Supervision** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision);

— **Supervision of Service in Cessation** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

— **Supervision Ceased** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— **Supervision Revoked** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked);

▼M1

— **Accredited** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited);

▼C1

— **Accreditation Ceased** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— **Accreditation Revoked** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

The above statuses SHALL be interpreted, in the context of the present specifications of the Trusted List as follows:

— ***Under Supervision:*** The service identified in 'Service digital identity' (clause 5.5.3) provided by the Certification Service Provider (CSP) identified in 'TSP name' (clause 5.4.1) is currently under supervision, for compliance with the provisions laid down in Directive 1999/93/EC, by the Member State identified in the 'Scheme territory' (clause 5.3.10) in which the CSP is established.

▼M1

— ***Supervision of Service in Cessation:*** The service identified in 'Service digital identity' (clause 5.5.3) provided by the CSP identified in 'TSP name' (clause 5.4.1) is currently in a cessation phase but still supervised until supervision is ceased or revoked. In the event a different legal person than the one identified in 'TSP name' has taken over the responsibility of ensuring this cessation phase, the identification of this new or fallback legal person (fallback CSP) SHALL be provided in 'Scheme service definition URI' (clause 5.5.6) and in the 'TakenOverBy' extension (clause L.3.2) of the service entry.

▼C1

— ***Supervision Ceased:*** The validity of the supervision assessment has lapsed without the service identified in 'Service digital identity' (clause 5.5.3) being re-assessed. The service is currently not under supervision any more from the date of the current status as the service is understood to have ceased operations.

— ***Supervision Revoked:*** Having been previously supervised, the CSP's service and potentially the CSP itself has failed to continue to comply with the provisions laid down in Directive 1999/93/EC, as determined by the Member State identified in the 'Scheme territory' (clause 5.3.10) in which the CSP is established. Accordingly the service has been required to cease its operations and must be considered as ceased for the above reason.

Note(1): The status value 'Supervision Revoked' can be a definitive status, even if the CSP then completely ceases its activity; there is no need to migrate to either 'Supervision of Service in Cessation' or to 'Supervision Ceased' status in this case. Actually, the only way to change the 'Supervision Revoked' status is to recover from non-compliance to compliance with the provisions laid down in Directive 1999/93/EC according to the appropriate supervision system in force in the Member State owing the TL, and regaining 'Under Supervision' status. 'Supervision of Service in Cessation' status, or 'Supervision Ceased' status only happens when a CSP directly ceases its related services under supervision, not when supervision has been revoked.

— ***Accredited:*** An accreditation assessment has been performed by the Accreditation Body on behalf of the Member State identified in the 'Scheme territory' (clause 5.3.10) and the service identified in 'Service digital identity' (clause 5.5.3) provided by the CSP [1] identified in 'TSP name' (clause 5.4.1) is found to be in compliance with the provisions laid down in Directive 1999/93/EC.

[1] Note that this accredited CSP may be established in another Member State than the one identified in the 'Scheme territory' of the TSL implementation of the TL or in a third country (see Art.7.1(a) of Directive 1999/93/EC).

▼C1

Note(2): When used in the context of a CSP issuing QCs that is established in the 'Scheme territory' (clause 5.3.10), the following two statuses 'Accreditation Revoked' and 'Accreditation Ceased' MUST be considered as 'transit statuses' and MUST not be used as value for 'Service current status' as, in case they are used, they MUST be immediately followed in the 'Service approval history information' or in the 'Service current status' by an 'Under supervision' status, potentially followed by any other supervision status defined here above and as illustrated in Figure 1. When used in the context of a CSP not issuing QCs when there is only an associated 'voluntary accreditation' scheme with no associated supervision scheme or in the context of a CSP issuing QCs where the CSP is not established in the 'Scheme territory' (clause 5.3.10) (e.g. in a third country), those 'Accreditation Revoked' and 'Accreditation Ceased' statuses MAY be used as a value for 'Service current status':

— ***Accreditation Ceased:*** The validity of the accreditation assessment has lapsed without the service identified in 'Service digital identity' (clause 5.5.3) being re-assessed.

— ***Accreditation Revoked:*** Having been previously found to be in conformance with the scheme criteria, the service identified in 'Service digital identity' (clause 5.5.3) provided by the Certification Service Provider (CSP) identified in 'TSP name' (clause 5.4.1)and potentially the CSP itself have failed to continue to comply with the provisions laid down in Directive 1999/93/EC.

Note(3): Exactly the same status values must be used for CSPs issuing QCs and for CSPs not issuing QCs (e.g. Time Stamping Service Providers issuing TSTs, CSPs issuing non-qualified certificates, etc.). The 'Service Type identifier' (clause 5.5.1) shall be used to distinguish between applicable supervision/accreditation systems.

Note(4): Additional status-related 'qualification' information defined at the level of national supervision/accreditation systems for CSPs not issuing QCs MAY be provided at the service level when applicable and required (e.g. to distinguish between several quality/security levels). Scheme Operators SHALL use the 'additionalServiceInformation' extension (clause 5.8.2) of the 'Service information extension' field (clause 5.5.9) according to the purpose of providing such additional 'qualification' information. Additionally, the Scheme operator can optionally use clause 5.5.6 (Scheme service definition URI).

Current status starting date and time (clause 5.5.5)

This field is REQUIRED and SHALL specify the date and time on which the current approval status became effective (date and time value as defined in ETSI TS 102 231 clause 5.1.4).

Scheme service definition URI (clause 5.5.6)

This field is OPTIONAL, and if present SHALL specify the URI(s) where relying parties can obtain service-specific information provided by the Scheme Operator as a sequence of multilingual pointers (with EN as the mandatory language and potentially with one or more national languages).

When used, the referenced URI(s) MUST provide a path to information describing the service as specified by the scheme. In particular this MAY include when applicable:

(a) URI indicating the identity of the fallback CSP in the event of the supervision of a service in cessation for which a fallback CSP is involved (see 'Service current status' — clause 5.5.4);

▼C1

(b) URI leading to documents providing additional information related to the use of some nationally defined specific qualification for a supervised/accredited Trust Service Token provisioning service in consistence with the use of 'Service information extension' field (clause 5.5.9) with an 'additionalServiceInformation' extension as defined in clause 5.8.2.

Service supply points (clause 5.5.7)

This field is OPTIONAL, and if present SHALL specify the URI(s) where relying parties can access the service through a sequence of character strings whose syntax MUST be compliant with RFC 3986.

TSP service definition URI (clause 5.5.8)

This field is OPTIONAL, and if present SHALL specify the URI(s) where relying parties can obtain service-specific information provided by the TSP as a sequence of multilingual pointers (with EN as the mandatory language and potentially with one or more national languages). The referenced URI(s) MUST provide a path to information describing the service as specified by the TSP.

Service information extensions (clause 5.5.9)

In the context of the present specifications, this field is OPTIONAL but SHALL be present when the information provided in the 'Service digital identity' (clause 5.5.3) is not sufficient to unambiguously identify the qualified certificates issued by this service and/or the information present in the related qualified certificates does not allow machine-processable identification of the facts about whether or not the QC is supported by an SSCD ([1]).

In the context of the present specifications, when its use is REQUIRED, e.g. for CA/QC services, an optional 'Service information extensions' (Sie) information field SHALL be used and structured, according to the 'Qualifications' extension defined in ETSI TS 102 231 Annex L.3.1, as a sequence of one or more tuples, each tuple providing:

— (filters) Information to be used to further identify under the 'Sdi' identified certification service that precise service (i.e. set of qualified certificates) for which additional information is required/provided with regard to the presence or absence of SSCD support (and/or issuance to Legal Person); and

— The associated information (qualifiers) about whether this further identified service set of qualified certificates is supported by an SSCD or not (when this information is 'QCSSCDStatusAsInCert', this means that this associated information is part of the QC under an ETSI standardised machine-processable form ([2])), and/or information regarding the fact that such QCs are issued to Legal Person (by default they are to be considered as only issued to Natural Persons).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): means that it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that any QC issued under the service (QCA) identified in 'Service digital identity' (clause 5.5.3) and further identified by the above (filters) information used to further identify under the 'Sdi' identified certification service that precise set of qualified certificates for which this additional information is required with regard to the presence or absence of SSCD support ARE supported by an SSCD (i.e. that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with Annex III of Directive 1999/93/EC);

([1]) See section 2.2 of the present document.

([2]) This refers to an appropriate combination of ETSI defined QcCompliance statement, QcSSCD statements [ETSI TS 101 862] or a QCP/QCP + ETSI defined OID [ETSI TS 101 456].

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD): means that it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that any QC issued under the service (RootCA/QC or CA/QC) identified in 'Service digital identity' (clause 5.5.3) and further identified by the above (filters) information used to further identify under the 'Sdi' identified certification service that precise set of qualified certificates for which this additional information is required with regard to the presence or absence of SSCD support ARE NOT supported by an SSCD (i.e. that the private key associated with the public key in the certificate is **not** stored in a Secure Signature Creation Device conformant with Annex III of Directive 1999/93/EC]).

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): means that it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that any QC issued under the service (CA/QC) identified in 'Service digital identity' (clause 5.5.3) and further identified by the above (filters) information used to further identify under the 'Sdi' identified certification service that precise set of qualified certificates for which this additional information is required with regard to the presence or absence of SSCD support SHALL contain the machine-processable information indicating whether or not the QC is supported by an SSCD;

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): means that it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that any QC issued under the service (QCA) identified in 'Service digital identity' (clause 5.5.3) and further identified by the above (filters) information used to further identify under the 'Sdi' identified certification service that precise set of qualified certificates for which this additional information is required with regard to the issuance to Legal Person **ARE** issued to Legal Persons.

Those qualifiers are only to be used as an extension, if the service type is http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

This field is implementation specific (ASN.1 or XML) and MUST comply with the specifications provided in ETSI TS 102 231, Annex L.3.1.

▼M1

In the context of an XML implementation, the specific content of such additional information has to be coded using the xsd files provided in Annex C of ETSI TS 102 231.

▼C1

Service Approval History

This field is OPTIONAL but MUST be present if 'Historical information period' (clause 5.3.12) is non-zero. Thus, in the context of the present specifications, the scheme MUST retain historical information. In the case where historical information is intended to be retained but the service has no history prior to the current status (i.e. a first recorded status or history information not retained by the scheme operator) this field SHALL be empty. Otherwise, for each change in TSP service current status which occurred within the historical information period as specified in ETSI TS 102 231 clause 5.3.12, information on the previous approval status SHALL be provided in a descending order of status change date and time (i.e. the date and time on which the subsequent approval status became effective).

▼C1

This SHALL be a sequence of history information as defined hereafter.

TSP(1) Service(1) History(1)

Service type identifier (clause 5.6.1)

This field is REQUIRED and SHALL specify the identifier of the service type, with the format and meaning used in 'TSP Service Information — Service type identifier' (clause 5.5.1).

Service name (clause 5.6.2)

This field is REQUIRED and SHALL specify the name under which the CSP provided the service identified in 'TSP Service Information — Service type identifier' (clause 5.5.1), with the format and meaning used in 'TSP Service Information — Service name' (clause 5.5.2). This clause does not require that the name be the same as that specified in clause 5.5.2. A change of name MAY be one of the circumstances requiring a new status.

▼M1

Service digital identity (clause 5.6.3)

This field is REQUIRED and SHALL specify at least one representation of the digital identifier (i.e. X.509v3 certificate) used in 'TSP Service Information — Service digital identity' (clause 5.5.3) with the format and meaning as defined in ETSI TS 102 231, clause 5.5.3.

Note: For an X.509v3 certificate value used in the 'Sdi' clause 5.5.3 of a service, there must be only one single service entry in a Trusted List per 'Sti:Sie/additionalServiceInformation' value. The 'Sdi' (clause 5.6.3) information used in the service approval history information associated to a service entry and the 'Sdi' (clause 5.5.3) information used in this service entry MUST relate to the same X.509v3 certificate value. When a listed service is changing its 'Sdi' (i.e. renewal or rekey of an X.509v3 certificate for e.g. a CA/PKC or CA/QC) or creating a new 'Sdi' for such a service, even with identical values for the associated 'Sti', 'Sn', and ['Sie'], it means that the Scheme Operator MUST create a different service entry than the previous one.

▼C1

Service previous status (clause 5.6.4)

This field is REQUIRED and SHALL specify the identifier of the previous status of the service, with the format and meaning used in 'TSP Service Information — Service current status' (clause 5.5.4).

Previous status starting date and time (clause 5.6.5)

This field is REQUIRED and SHALL specify the date and time on which the previous status in question became effective, with the format and meaning used in 'TSP Service Information — Service current status starting date and time' (clause 5.5.5).

Service information extensions (clause 5.6.6)

This field is OPTIONAL and MAY be used by scheme operators to provide specific service-related information with the format and meaning used in 'TSP Service Information — Service information extensions' (clause 5.5.9).

▼C1

TSP(1) Service(1) History(2)

Idem for TSP(1) Service(1) History(2) (prior to History 1)

…

TSP(1) Service(2)

Idem for TSP(1) Service 2 (as applicable)

TSP(1)Service(2)History(1)

…

TSP(2) Information

Idem for TSP 2 (as applicable)

Idem for TSP 2 Service 1

Idem for TSP 2 Service 1 History 1

…

▼M1

Signed TSL

The human readable TSL implementation of the Trusted List, established under the present specifications and in particular Chapter IV, SHOULD be signed by the 'Scheme operator name' (clause 5.3.4) to ensure its authenticity and integrity ([1]). The format of the signature SHOULD be PAdES part 3 (ETSI TS 102 778-3 ([2])) but MAY be PAdES part 2 (ETSI TS 102 778-2 ([3])) in the context of the specific trust model established through the publication of the certificates used to sign the Trusted Lists.

The machine processable TSL implementation of the Trusted List, established under the present specifications, SHALL be signed by the 'Scheme operator name' (clause 5.3.4) to ensure its authenticity and integrity. The format of the machine processable TSL implementation of the Trusted List, established under the present specifications, SHALL be XML and SHALL comply with the specifications stated in Annexes B and C of ETSI TS 102 231.

The format of the signature SHALL be XAdES BES or EPES as defined by ETSI TS 101 903 specifications for XML implementations. Such electronic signature implementation SHALL meet requirements as stated in Annex B of ETSI TS 102 231 ([4]). Additional general requirements regarding this signature are stated in the following sections.

▼C1

Scheme identification (clause 5.7.2)

This field is REQUIRED and SHALL specify a reference assigned by the scheme operator which uniquely identifies the scheme described in the present specifications and the established TSL, and MUST be included in the calculation of the signature. This is expected to be a character string or a bit string.

([1]) In case the human readable TSL implementation of the Trusted List is not signed, its authenticity and integrity MUST be guaranteed by an appropriate communication channel with an equivalent security level. Use of TLS (IETF RFC 5246: 'The Transport Layer Security (TLS) Protocol Version 1.2') is recommended for this purpose and the fingerprint of the certificate of the TLS channel MUST be made available out of band to the TSL users by the Member State.

([2]) ETSI TS 102 778-3 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced — PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic — Profile based on ISO 32000-1.

([4]) It is mandatory to protect the Scheme Operator signing certificate with the signature in one of the ways specified by ETSI TS 101 903 and the ds:keyInfo should contain the relevant certificate chain when applicable.

▼M1

In the context of the present specifications the assigned reference SHALL include the 'TSL type' (clause 5.3.3), the 'Scheme name' (clause 5.3.6) and the value of the SubjectKeyIdentifier extension of the certificate used by the Scheme operator to electronically sign the TSL.

▼C1

Signature algorithm identifier (clause 5.7.3)

This field is REQUIRED and SHALL specify the cryptographic algorithm that has been used to create the signature. Depending on the algorithm used, this field MAY require additional parameters. This field MUST be included in the calculation of the signature.

Signature value (clause 5.7.4)

This field is REQUIRED and SHALL contain the actual value of the digital signature. All fields of the TSL (except the signature value itself) MUST be included in the calculation of the signature.

TSL extensions (clause 5.8)

expiredCertsRevocationInfo Extension (clause 5.8.1)

This extension is OPTIONAL. When used it MUST comply to the specifications of ETSI TS 102 231, clause 5.8.1.

additionalServiceInformation Extension (clause 5.8.2)

This OPTIONAL extension, when used, MUST be used at Service level only and only in the field defined in clause 5.5.9 (Service information extension). It is used to provide additional information on a service. This SHALL be a sequence of one or more tuples, each tuple giving:

(a) an URI identifying the additional information, e.g.:

— an URI indicating some nationally defined specific qualification for a supervised/accredited Trust Service Token provisioning service, e.g.

— a specific security/quality granularity level with regard to national supervision/accreditation scheme for CSPs not issuing QCs (e.g. RGS */**/*** in FR, specific 'supervision' status set by national legislation for specific CSPs issuing QCs in DE), see Note(4) of 'Service current status' — clause 5.5.4;

— or a specific legal status for a supervised/accredited Trust Service Token provisioning (e.g. nationally defined 'qualified TST' as in DE or HU);

— or meaning of a specific Policy identifier present in a X.509v3 certificate provided in 'Sdi' field.

— or a registered URI as specified in 'Service type identifier', clause 5.5.1, in order to further specify the participation of the 'Sti' identified service as being a component service of a certification service provider issuing QC (e.g., OCSP-QC, CRL-QC, and RootCA-QC);

(b) an optional string containing the serviceInformation value, meaning as specified in the scheme (e.g. *, ** or ***);

(c) any optional additional information provided in a scheme-specific format.

▼**M1**

Dereferencing the URI SHOULD lead to human readable information (as a minimum in EN and potentially in one or more national languages) which is deemed appropriate and sufficient for a relying party to understand the extension, and in particular explaining the meaning of the given URIs, specifying the possible values for serviceInformation and the meaning for each value.

Qualifications Extension (clause L.3.1)

Description: This field is OPTIONAL but SHALL be present when its use is REQUIRED, e.g. for RootCA/QC or CA/QC services, and when

— the information provided in the 'Service digital identity' is not sufficient to unambiguously identify the qualified certificates issued by this service,

— the information present in the related qualified certificates does not allow machine-processable identification of the facts about whether or not the QC is supported by an SSCD.

When used, this service level extension MUST only be used in the field defined in 'Service information extension' (clause 5.5.9) and SHALL comply with specifications laid down in Annex L.3.1 of ETSI TS 102 231.

TakenOverBy Extension (clause L.3.2)

Description: This extension is OPTIONAL but SHALL be present when a service that was formerly under the legal responsibility of a CSP is taken over by another TSP and is meant to state formally the legal responsibility of a service and to enable the verification software to display to the user some legal detail. The information provided in this extension SHALL be consistent with the related use of clause 5.5.6 and SHALL comply with specifications in Annex L.3.2 of ETSI TS 102 231.

▼M1

CHAPTER II

When establishing their Trusted Lists, Member States will use:

Language codes in lower case and country codes in upper case;

Language and country codes according to the Table provided here below.

When a Latin script is present (with its proper language code) a transliteration in Latin script with the related language codes specified in the Table below is added.

Short name (source language)	Short name (English)	Country Code	Language Code	Notes	Transliteration in Latin script
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	Country code recommended by EU	el-Latn
España	Spain	ES	es	also Catalan (ca), Basque (eu), Galician (gl)	
France	France	FR	fr		
▼M2 Hrvatska	Croatia	HR	Hr		
▼M1 Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼M1

Short name (source language)	Short name (English)	Country Code	Language Code	Notes	Transliteration in Latin script
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Country code recommended by EU	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Latin transliteration: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

CHAPTER IV

SPECIFICATIONS FOR THE HUMAN READABLE FORM OF THE TSL IMPLEMENTATION OF THE TRUSTED LIST

A Human Readable (HR) form of the TSL implementation of the Trusted List MUST be publicly available and accessible by electronic means. It SHOULD be provided in the form of a Portable Document Format (PDF) document according to ISO 32000 that MUST be formatted according to the profile PDF/A (ISO 19005).

The content of the PDF/A based HR form of the TSL implementation of the Trusted List SHOULD comply with the following requirements:

▼M1

— The title of the Human readable form of Trusted Lists shall be constructed as the concatenation of the following elements:

  — Optional picture of the Member State national flag;

  — Blank space;

  — Country Short Name in source language(s) (as provided in the first column of Chapter II Table);

  — Blank space;

  — ‘(’;

  — Country Short Name in English (as provided in the second column of Chapter II Table) inside the parenthesis;

  — ‘):’ as closing parenthesis and separator;

  — Blank space;

  — ‘Trusted List’;

  — Optional logo of the Member State Scheme Operator;

▼C1

— The structure of the HR form SHOULD reflect the logical model described in section 5.1.2 of ETSI TS 102 231;

— Every present field SHOULD be displayed and provide:

  — The title of the field (e.g. ‘Service type identifier’);

  — The value of the field (e.g. ‘CA/QC’);

  — The meaning (description) of the value of the field, when applicable and in particular as provided in Annex D of ETSI TS 102 231 or in the present specifications for registered URIs (e.g. ‘A Certification authority issuing public key certificates.’);

  — Multiple natural languages versions as provided in the TSL implementation of the Trusted List, when applicable.

— The following fields and corresponding values of the digital certificates present in the ‘Service digital identity’ field SHOULD be at a minimum displayed in the HR form:

  — Version,

  — Serial number,

  — Signature algorithm,

  — Issuer,

  — Valid from,

  — Valid to,

  — Subject,

▼C1

— Public key,

— Certificate Policies,

— Subject Key Identifier,

— CRL Distribution Points,

— Authority Key Identifier,

— Key Usage,

— Basic constraints,

— Thumbprint algorithm,

— Thumbprint,

— The HR form SHOULD be easily printable,

— The HR form MAY be signed electronically. When signed it MUST be signed by the Scheme Operator according to the same signature specifications as for the TSL implementation of the Trusted List.