Study on Cross-Border Interoperability of eSignatures

(CROBIES)

"Trusted Lists"

Implementer's Guide

A report to the European Commission

from SEALED, time.lex and Siemens

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

FINAL REPORT

Editing company: SEALED sprl,
VAT: BE 0876.866.142 – RPM: Tournai
12, rue de la Paix, B-7500 Tournai
olivier.delos@sealed.be, sylvie.lacroix@sealed.be

Date: 31/07/2010
Version: 1.0

Document information

Title:	CROBIES Work Package 2-1 **Trusted Lists – Implementer's Guide**
Project reference:	CROBIES
Document archival code:	INFSO-CROBIES-FINALREPORT-WP2-1-SEALED-31072010_v1

Version control

Version	Date	Description / Status	Responsible
V1.0	31/07/2010	Final report	ODO, SLR

References

Reference	Title
[1]	The European **Directive 1999/93/EC** of the European Parliament and the Council of the 13 December 1999 on a Community framework for electronic signatures. O.J. L 13, 19.1.200, p.12.
[2]	**Study on the standardisation aspects of eSignature**. A study for the European Commission (DG Information Society and Media) by SEALED, DLA Piper and Across communications, 22/11/2007.
[3]	**Commission Decision 2003/511/EC** "on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the EP and the Council". OJ L 175 15.7.2003, p.45.
[4]	**Services Directive 2006/123/EC** of the European Parliament and of the Council of 12 December 2006 on services in the internal market. OJ L 376, 27.12.2006, p. 36.
[5]	**ETSI TS 102 231 v3.1.2** (2009-12): Electronic Signatures and Infrastructures (ESI); Provision of harmonised Trust-service status information.
[6]	**Corrigendum to Commission Decision 2009/767/EC** 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. *(Official Journal of the European Union L 299 of 14 November 2009)*.
[7]	**Commission Decision 2010/425/EU** of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States (OJ L 199 of 31.07.2010).
[8]	**Mandate M460**, Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies applied to electronic signatures, 7 January 2010.
[9]	**TSL contents for the TSL lifecycle test cases**, J. C. Cruellas (UPC), Olivier Delos (SEALED), November 2009, © 2009 ETSI.

Definitions and Acronyms

Please refer to the CROBIES Head Document for definitions and acronyms used throughout the present report.

Table of Contents

Trusted Lists

Implementer's Guide

1 Introduction

1.1 CROBIES

The CROBIES study looks at eSignature interoperability in general, but specifically in the context of cross-border use. While considering a consistent global and long term approach in proposed improvements at the legal, technical and trust levels, CROBIES is also focusing on quick wins that could substantially improve the interoperability of electronic signatures.

The CROBIES Study concentrates in particular on the following aspects through related work packages and their associated reports:

WP1. The proposal for a common model for supervision and accreditation systems of certification service providers (CSPs) issuing QCs (and other services ancillary to electronic signatures);

WP2. The establishment of a "Trusted List of supervised/accredited Certification Service Providers" (in particular issuing QCs);

WP3. Interoperable profiles of qualified certificates issued by supervised/accredited CSPs in Member States;

WP4. A proposed framework for interoperable Secure Signature Creation Devices (SSCDs); and

WP5. A proposed model for providing guidelines and guidance for cross-border and interoperable implementation of electronic signatures.

The global overview of the CROBIES study and of its approach is to be found in the "Head Document" of the study. The study is part of the *Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market* adopted by the European Commission on 28.11.2008[1] which aims at facilitating the provision of cross-border public services in an electronic environment. Readers are suggested to read this Head Document prior to reading the present report.

1.2 Target Audience

The present report is mainly addressed to Member State Supervisory Bodies in charge of the appropriate supervision of certification service providers established on their territory and issuing qualified certificates, as well as to those similar Supervisory and/or Accreditation Bodies in charge of the approval, supervision, and/or accreditation of any type of CSP providing services ancillary to electronic signatures, e.g. issuing certificates or providing other services related to electronic signatures for which a national approval scheme is in place.

[1] COM(2008) 798, http://ec.europa.eu/information_society/policy/esignature/action_plan/index_en.htm.

The present report is also addressed to the ESO's to support their work in the context of the eSignature Mandate M460 [8], and to any interested electronic signature stakeholder or third party.

1.3 Executive Summary

Work Package 2 (WP2) of the CROBIES Study analyses the "Trusted List" concept for providing information on the supervision/accreditation status of certification services (e.g. issuing Qualified Certificates) from Certification Service Providers (CSPs) that are supervised/accredited by Member States, notably for compliance with the provisions laid down in Directive 1999/93/EC [1]. This covers the structure and content of *(a common template for)* the Trusted List of a Member State, its publication modes, its establishment and life-cycle management, and its use. CROBIES also provided support to the implementation of the "European Commission Compiled List of links towards national Trusted Lists established in the EU Member States". This compiled list (also called the List of the Lists – LOTL) provides the required information to reach those national Trusted Lists further facilitating the validation process of electronic signatures based on qualified certificates on a European scale.

The need for Trusted Lists (TL) comes from the fact that in practice several difficulties linked to the use of Qualified Electronic Signatures (QES) and Advanced electronic Signature based on Qualified Certificates ($AdES_{QC}$), especially in a cross-border use, still persist and needed to be solved. This includes issues linked to the trust on e-signatures originating from other Member States. Such trust could be improved by making available information on the supervision/accreditation status of the certification services issuing Qualified Certificates (QC) from CSPs established or accredited in Member States. This information is essential to support the validation of QES and AdES supported by QC in a cross-border context. The Member States' national Trusted List[2] defined in Decision 2009/767/EC [6] amended by Decision 2010/425/EU [7] aim to further support the interoperability and to facilitate the cross-border use of e-signatures, through a common template and format of Trusted Lists.

Indeed, on the one hand, the data contained in the certificate should allow validating the fact that the certificate is indeed a QC and whether it is supported by a Secure Signature Creation Device (SSCD) in case of a QES. Unfortunately, today relying on the signatory's certificate (path) may not be enough to get the needed data or it is too complicated (e.g. not machine processable, or sometimes not even manually feasible), due to a number of differences in current requirements and practices linked to the issuance and use of QC in Member States[3]. Therefore at this stage this information should be available through other means, namely the Trusted List. The Trusted List of the Member State in which the Certification Service Provider (CSP) issuing the signatory's certificate is established or accredited should assist the receiving party to receive the confirmation of the supervision / accreditation status of the certification service having issued the claimed QC supporting the received electronic signature, and when required to receive the required statement with regards to the qualified status of the certificate and/or whether it is supported by a SSCD when such information is not appropriately provided in the QC. This information

[2] 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".

[3] Differences in the actual content of QC issued by CSPs issuing QCs, varying legal requirements for QC profiles, the use of different standards and the wide degree of interpretation of those standards as well as the unawareness of the existence and precedence of some normative technical specifications or standards.

complements the information in the signatory's certificate (chain) supporting an electronic signature.

On the other hand the Trusted Lists provides trustworthy information about the supervision / accreditation status of the certification services (e.g. issuing qualified certificates) from CSPs that are supervised / accredited by Members States for compliance with the relevant provisions of Directive 1999/93/EC. This brings confidence in the fact that a certificate supporting a claimed QES or $AdES_{QC}$ is indeed issued by a listed service from a supervised or accredited CSP and on the fact that it is indeed a QC and whether or not it is supported by an SSCD (whether those CSP statements are part of the certificate or the information is provided in the Trusted List itself).

The rationale for the genesis of Trusted Lists and the related CD 2009/767/EC is provided in Annex 1 of the present report.

The Trusted Lists specifications can easily be found in the following documents to the elaboration of which the CROBIES team significantly contributed in the context of WP2:

- Commission Decision 2009/767/EC [6] amended by Decision 2010/425/EU [7] setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC on services in the internal market [4];[4]
- ETSI TS 102 231 v3.1.2 [5][5] on which the Trusted List technical specifications provided in annexes of Decisions 2009/767/EC and 2010/425/EU are based;
- The European Commission web page from where information on and latest instance of the compiled list of links towards the Member States national Trusted List can be found.[6]

Since the finalisation of CD 2009/767/EC [6] late 2009, a number of practical tests with the European Telecommunications Standards Institute (ETSI) have been organised to allow Member States to check the conformity of their Trusted Lists with the specifications set out in the Annex to Decision 2009/767/EC. These tests have demonstrated that some technical changes were needed in the technical specifications in the Annex to Decision 2009/767/EC, to ensure functioning and interoperable trusted lists, and also confirmed the need for Member States to make publicly available not only the human readable versions of their trusted lists as required by Decision 2009/767/EC but also the machine processable forms of these, facilitating their use by allowing for their automated processing and thereby enhance their use in public electronic services. In order to facilitate access to the national Trusted Lists, Member States should notify to the Commission information related to the location and protection of their trusted lists. This information should be made available by the Commission to other Member States in a secure manner, in practice through the Compiled List (LOTL).

Decision 2009/767/EC [6] should therefore be amended accordingly through an amendment that has been published in the Official Journal under Decision 2010/425/EU while the required technical changes to the national Trusted List should apply as of 1 December 2010 for the purpose of allowing Member States to carry out those changes [7].

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN:PDF
[5] http://pda.etsi.org/pda/home.asp?wki_id=KKdPr7fB0zBECKFG7I7bZ
[6] http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm

The compiled provisions and technical requirements from CD 2009/767/EC as amended by Decision 2010/425/EU [7] are provided as an unabridged version for information purposes in Annex 2 of the present report.

The aim of the present report "Trusted Lists – Implementer's Guide" is to provide a general guidance on how Trusted Lists should be established content wise as well as on the associated trust model as set-up by the amendment on Decision 2009/767/EC [6][7]. This document can be seen as a FAQ for Member State Scheme Operator (and/or Supervisory Body and/or Accreditation Body) when establishing their national Trusted List.

Section 2 describes the scope of Trusted Lists, the structure of the common template used to establish them through specific guidance, explanations and sometimes clarifications on specifications stated in CD 20009/767/EC [6] as amended by Decision 2010/425/EU [7]. It also discusses the Trusted List trust model and Trusted Lists signatures. Specific cases that may occur during maintenance of Trusted List are also elaborated as well as references to further technical aspects related to the implementation of Trusted Lists.

Finally Section 3 proposes yet some changes to the amended version of CD 2009/767/EC [6] [7] for further clarification and simplification.

2 Trusted Lists

2.1 Scope of the Trusted Lists

The Trusted Lists of supervised/accredited Certification Service Providers, through a common template and rules defined in CD 2009/767/EC [6] amended by Decision 2010/425/EU [7], aim 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[7] (CSPs) who are supervised/accredited by them, notably for compliance with the relevant provisions of Directive 1999/93/EC [1]. This includes the provision of historical information about the supervision/accreditation status of the supervised/accredited certification services.

As depicted in Figure 1 below, one single list must be established, published and maintained per Member State providing information on supervision/accreditation status both of certification services issuing qualified certificates and, on a voluntary basis, of any other certification services related or ancillary to electronic signatures for compliance with the relevant provisions of Directive 1999/93/EC.

[7] As defined in Art. 2.11 of Directive 1999/93/EC.

Trusted List of supervised/accredited CSPs

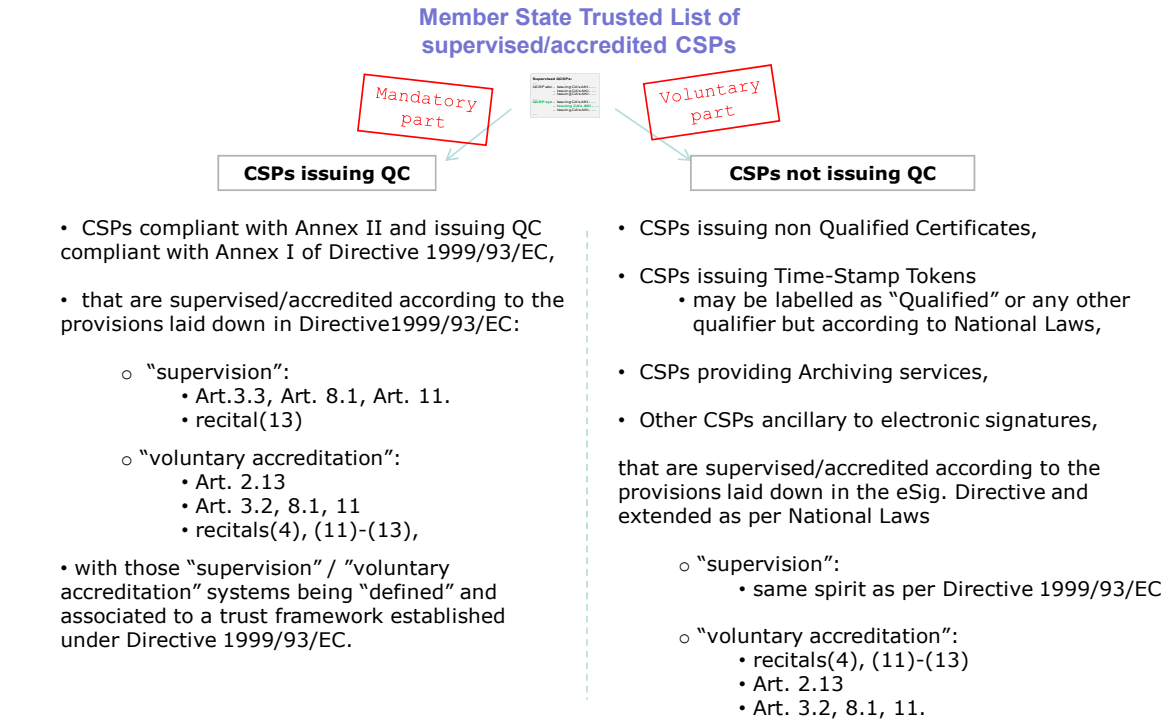


Figure 1

The Trusted List of a Member State 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**, notably 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 the Member State in which they are established, which may differ from the

Member State in which they are accredited, unless they are not established in a Member State but in a third country.

- The applicable 'supervision' system (respectively 'voluntary accreditation' system) 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.

The mandatory information in the Trusted List (TL) must include a minimum of information on supervised/accredited CSPs issuing Qualified Certificates (QCs)[8] 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)[9].

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.

As a general principle the Trusted List is organised per Certification Service Provider and then per service from those listed CSPs. On a per service basis, a clear distinction is made between the services types in order to identify whether it is a certification service issuing QC (CA/QC), a certification service issuing non-qualified public key certificates (CA/PKC), or an OCSP service, a CRL issuing service or even a Time Stamping service, etc. The supervision/accreditation status information (and its related history) is given on a per service basis according to a defined status set of values and flow as illustrated in Figure 2.

[8] As defined in Art. 2.10 of Directive 1999/93/EC.
[9] As defined in Art. 2.6 of Directive 1999/93/EC.

Expected supervision/accreditation status flow for a single CSP service

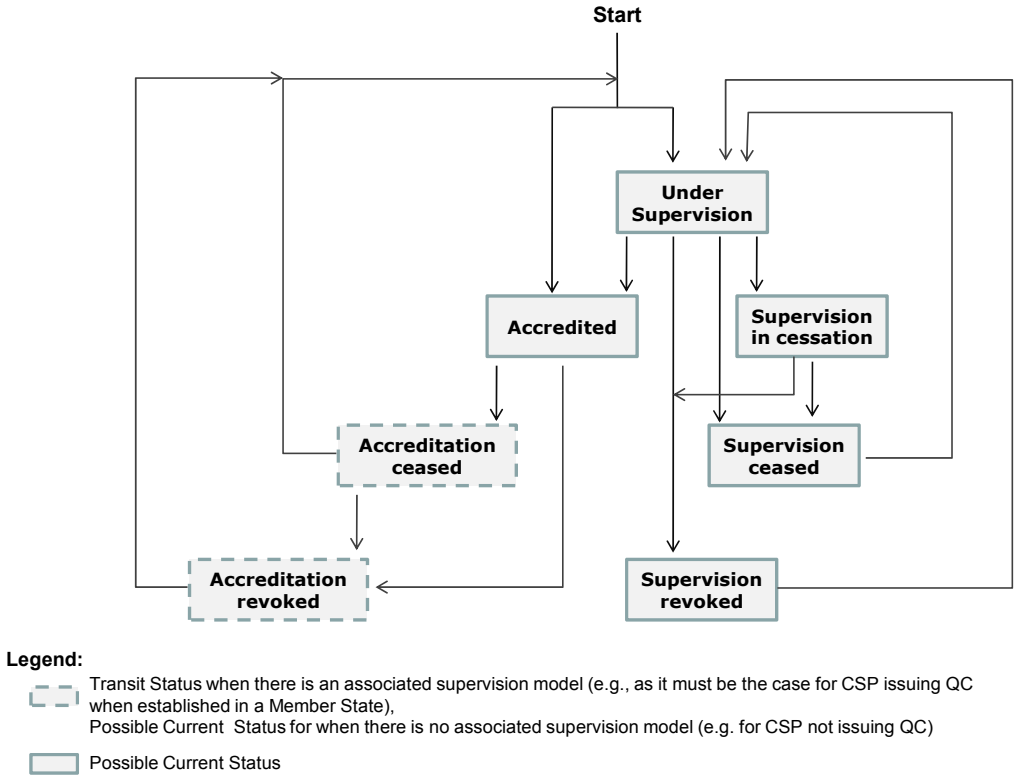


Figure 2

The meaning of those status values is a function of the type of service and of the associated supervision/accreditation system. The definition and scope information applicable to those supervision/accreditation systems are provided in the Trusted List at a list level and when applicable and on a national basis, for certification services not issuing qualified certificates, at a service level in order to allow indication of sub-levels of supervision/accreditation status[10].

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, e.g. with regards of certification services issuing qualified certificates by allowing the verification of the "qualified" status of a certificate and of its potential support by an SSCD.

[10] E.g. RGS one-, two-, or three-star level for certification services issuing public key certificates is France. More information on the Référentiel Général de Sécurité (RGS) or General Security Directory (GSD) on http://www.ssi.gouv.fr/

In particular, this information is aimed primarily at supporting the validation of Qualified Electronic Signatures (QES) and Advanced Electronic Signatures (AdES)[11] supported by a Qualified Certificate[12,13].

The Technical Specifications for the Trusted List's Common Template, as part of CD 2009/767/EC [6] amended by Decision 2010/425/EU [7], are fully compliant with, and can be considered as a profile of, the ETSI Technical Specifications TS 102 231 v3.1.2 [5] for the provision of harmonised Trust-service status information through the usage of so-called Trust-service Status Lists (TSL) that can be used to address the establishment, publication, location, access, authentication and trusting of such kinds of lists.

2.2 Structure of the common template for the Trusted Lists

The Common Template for a Member State Trusted List is 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**;

[11] As defined in Art. 2.2 of Directive 1999/93/EC [1].
[12] For an AdES supported by a QC the acronym "$AdES_{QC}$" is used throughout the present document.
[13] 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.

- 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);
- 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).

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.

2.2.1 **Owner of the TSL implementation**

The TSL implementation of a Member State Trusted List shall specify the name and coordinates of the Member State's Body in charge of establishing, publishing and maintaining the National Trusted List (i.e. The Scheme operator name, clause 5.3.4 of CD 2009/767/EC Annex [6] amended by Decision 2010/425/EU [7]). 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.

A country may have separate Supervisory and Accreditation Bodies and even additional bodies for whatever operational related activities. It is then up to each Member State to designate the Scheme operator of the TSL implementation of the Member State Trusted List. It is expected that the Supervisory Body, the Accreditation Body and the Scheme Operator (when they appear to be separate bodies) will have, each of them, 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 Trusted List, including in the scheme-specific information indicated by the "Scheme information URI" (clause 5.3.7 of [6][7]).

The named Scheme Operator (clause 5.3.4 of [6][7]) is the entity who will sign the TSL implementation of the Trusted List.

The Trusted List specifications also foresee provision of contact information for the Scheme Operator, namely postal address information and electronic address information (i.e. email and/or website URI). When a Member State is willing to provide phone communication facilities (e.g. service help line capability) with regards to communication facilities with the Scheme Operator, it should use the content of a referenced web-site URI as part of the Scheme operator electronic address (clause 5.3.5.2 of [6][7]). When a Member State is willing to provide phone communication facilities (e.g. service help line capability) with regards to communication facilities with the Scheme Operator, Member State should use the content of a referenced web-site URI as part of the Scheme operator electronic address (clause 5.3.5.2 of [6][7]).

2.2.2 **Information on the supervision/accreditation schemes underlying the Trusted List**

The TSL implementation of a Member State Trusted List shall contain a specific name[14] identifying the TSL as a Trusted List and references (URIs) from which users (relying parties)

[14] "Scheme name" (clause 5.3.6 [6][7]), see annex 2 for further details on the format of such a name.

can obtain scheme-specific information[15]. The referenced URI(s) must provide a path to information describing appropriate information about the supervision / accreditation "scheme" that is underlying the TSL entries and the status information about the listed certification services and their meaning.

This "appropriate information about the scheme" provided in the TSL implementation of the Trusted List is organised through the use of the following fields (or clauses) of the Trusted List template:

- The "Scheme name" (clause 5.3.6 [6][7]);
- The "Scheme information URI (clause 5.3.7 [6][7]);
- The "Scheme type/community/rules" (clause 5.3.9 [6][7]);
- The "TSL policy/legal notice" (clause 5.3.11 [6][7]).

Scheme name

The Scheme Name value is the same for all Member State Trusted Lists (whether they are listing services related to the issuance of QCs only or other services as well), being the English value defined in the Amendment [7] of CD 2009/767/EC [6], potentially translated in as many national languages as required by a Member State.

Scheme information URI

This clause is used to provide 'appropriate information about the scheme', i.e. about the Member State "approval scheme(s)" underlying the Member State Trusted List.

It is a sequence of one or more URIs. English version is mandatory and national languages versions are optional. This can be implemented in only one URI but more likely through as many URI as there are languages used.

All language versions shall contain the mandatory text as defined in CD 2009/767/EC [6], L 299/32 (being the text starting with "The present list …" and finishing with "…at a national level on a voluntary basis." – basically the first half of L 299/32 page) in which the four occurrences of "[*name of the relevant Member State*]" must be replaced by the name of the relevant Member State.

All language versions shall contain, in addition to the above referenced mandatory text, the following items:

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

[15] Note that as for any other human readable information provided to users of TSL implementation of Trusted Lists, this information must be provided in English as the mandatory language and with potentially one or more national languages when applicable.

> (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).

All Member States shall then include in all applicable language versions specific information on the supervision system (and if applicable, national voluntary accreditation system) for CSP issuing QC **and**, when listing any CSP not issuing QCs, the applicable supervision system or accreditation system. That specific information shall at least include the information described in the last three bullets as displayed before the footnote above.

When applicable the following must also be provided:

> — 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.

Optionally, and on a voluntary basis, MS can additionally provide

> — 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.

This way of using the "Scheme information URI" clause is a first (mandatory) way for a Member State to provide information on its supervision system for CSP_{QC} and on its national approval scheme (supervision and/or accreditation) underlying the status determination of any listed service not being related to certification services issuing QCs but to any supervised/accredited certification services providing other services related, ancillary to electronic signatures (e.g. time-stamping services, archiving services, registered electronic mail).

Scheme type/community/rules

This field shall contain at least the following two URIs:

1. http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common
2. 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)

Dereferencing the first URI allows users to obtain a text common and applicable to all Member States Trusted Lists[16] (i) by which participation of the Member State's Trusted List is denoted as part of a scheme of schemes (i.e. the Compiled List pointing to all Member States Trusted Lists), (ii) where users can obtain policy/rules against which services included

[16] See CD 2009/767/EC [6] or by dereferencing the first URI.

in the list shall be assessed, (iii) where users can obtain a description about how to use and interpret the content of the TSL implementation of the Trusted List (usage rules which are common to all Member State Trusted Lists whatever the type of listed service and whatever the supervision/accreditation systems are.

Dereferencing the second URI shall allow users to:

> — […] 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.
>
> — […] 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.

Namely the second URI can be used by Member States to further explain the application of the content of the first URI in the Member Sate (in the event this is necessary and applicable) and in particular to provide for services not issuing QCs similar information as it is provided in the first URI for service issuing QC with regards to the interpretation of those services being listed in the TL and what would be the meaning the potential specific values for the services as per the potential granularity used in the "Service information extension" field.

It should be noted that 'Member States MAY define additional URIs from the above Member State specific URI (i.e. URIs defined from this hierarchical specific URI)' and that that any information obtained from these URIs shall be provided at least in English and potentially in any other national language as wished by the MS.

The applicable text or redirection value for content to be associated with the ETSI pre-registered country specific *schemerules* URI (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC) should be communicated to ETSI through the European Commission acting as a central communication point between Member States and ETSI according to a EC defined procedure.

TSL policy/legal notice

This field is made of text information for which the English version is mandatory (being the English text provided in CD 2009/767/EC [6]) and an optional part being a free text determined by the Member State.

As an example in the case of France (FR):

```
<tsl:PolicyOrLegalNotice>
  <tsl:TSLLegalNotice xml:lang="en">The applicable legal framework for the present TSL
     implementation of the Trusted List of supervised/accredited Certification Service
     Providers for FRANCE 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 FRANCE laws. The 2005-1516 ordinance and
     the RGS decree (which is currently being analysed by the State Council) define the
     accreditation scheme for all CSPs issuing qualified or non-qualified
     certificates.</tsl:TSLLegalNotice>
  <tsl:TSLLegalNotice xml:lang="fr">Le cadre légal applicable pour la présente
     implémentation de la TSL de la Liste de Confiance des Prestataires de Services de
     Confiance électronique supervisés/accrédités est la Directive 1999/93/EC du
     Parlement Européen et du Conseil du 13 décembre 1999 pour un cadre
     Communautaire pour la signature électronique et son implémentation selon la
```

législation Française. L'ordonnance 2005-1516 et le décret Référentiel Général de Sécurité (RGS) (en cours d'analyse au Conseil d'Etat) définissent le schéma d'accréditation pour tous les Prestataires de Services de Certification électronique émettant des certificats qualifiés ou non.</tsl:TSLLegalNotice>
</tsl:PolicyOrLegalNotice>

One can notice the black mandatory part and the specific green part for France (FR).

2.2.3 Historical information period

The TSL implementation of the Member State's Trusted List must contain historical information for a minimum of 10 years, i.e. a minimum of 3653 days.

2.2.4 Pointers to other TSLs

In order to allow access to the Trusted Lists of all Member States in an easy manner, the European Commission has published a central list, hereafter the "Compiled List", with links to national Trusted Lists.

The TSL implementation of the Member State's Trusted List must contain a pointer towards the European Commission Compiled List of pointers to all Member States Trusted Lists, including the digital identity X509.v3 certificate used by the European Commission to sign this Compiled List.

Article 2.(3)(4) of the amended version [7] of CD 2009/767/EC [6] is organising the Trust Model for Member States Trusted Lists signatures in such a way that the European Commission is making available, both in a human readable form and in a signed machine processable form, to all Member States, through a secure channel to an authenticated web server, the following information as notified by Member States:

> *"(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)."*

The authenticity and integrity of the machine processable version and of the human readable version of the Compiled List are ensured respectively through an electronic signature supported by a digital certificate and through a TLS/SSL secured connection supported by a digital certificate.[17]

[17] The latest certificates in use can be found through the European Commission Trusted List web page (http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm).
The current version of the machine processable signing certificate was published on page 16 of the Official Journal of the European Union C 45 of 23.02.2010 (http://eur-lex.europa.eu/Notice.do?checktexts=checkbox&val=508535:cs&pos=1&page=1&lang=en&pgs=10&nbl=1&list=508535:cs,&hwords=&action=GO&visu=#texte).

The authenticity and integrity of the Compiled List, and of the national Trusted Lists, should be verified by relying parties prior to any use.

2.2.5 List issue date/time and Next Update

The “List issue date and time” field specifies the date and time (UTC expressed as Zulu) on which the TSL implementation of the Trusted List was issued.

The “Next update” field specifies the latest date and time (UTC expressed as Zulu) by which the next TSL implementation of the Trusted List will be issued in the event that no earlier updated version of the TSL would need to be issued by then.

In the event of any change requiring the issuing of a new version of the TSL implementation of the Trusted List, the following must happen accordingly:

- Implementation of the required change(s);
- Increment of the “TSL sequence number”;
- Update the “List issue date and time”;
- And optionally update the “Next update” date and time.

In all case the difference between the “Next update” date and time and the “List issue date and time” value must not exceed 6 months.

In the event of no interim status change to any of the TSP services covered by the Trusted List and of no other change requiring its update, the TSL implementation of the Trusted List must be re-issued by the time of expiration of last TSL issued.

2.2.6 Listed TSPs

Trusted Lists’ content with regards to the supervision or accreditation status information about supervised or accredited services is organized per TSP, i.e. per legal entity providing such services. As illustrated in Figure 3 below, the list of TSPs is to be organised in such a way that 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).

The current version of the TSL/SSL certificate was published on page 15 of the Official Journal of the European Union C 57 of 09.03.2010 http://eur-lex.europa.eu/Notice.do?checktexts=checkbox&val=509136:cs&pos=1&page=1&lang=en&pgs=10&nbl=1&list=509148:cs,&hwords=&action=GO&visu=#texte

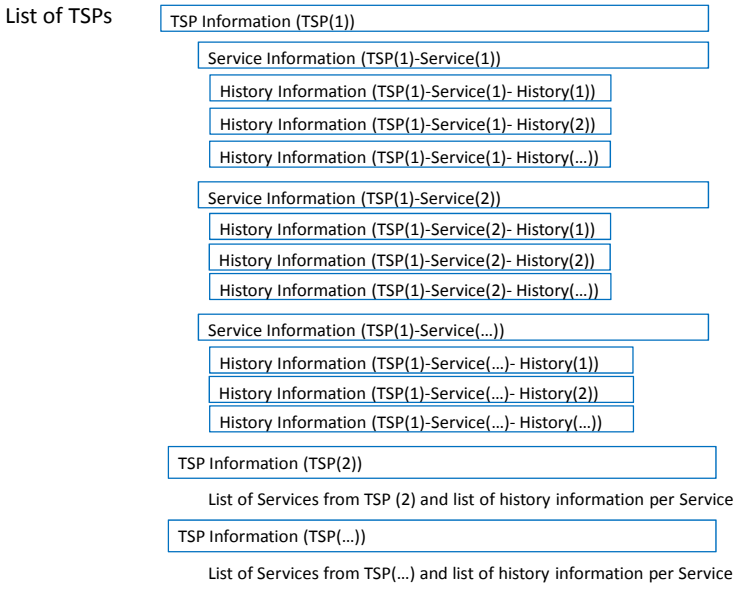


Figure 3

When there is no supervised or accredited TSP service in a Member State, there must be a TSL implementation of the Trusted List but this part of the Trusted List must be left empty. CD 2009/767/EC requires indeed that even when a Member State has no CSP either supervised or accredited by the scheme, Member States shall implement a TSL with this "List of Trust Service Providers" 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 above Figure 3).

The TSP information to be provided is made of the following fields: TSP name, TSP trade name (optional), TSP address, TSP information URI, and TSP information extensions (optional). Specifications for these fields are given in CD 2009/767/EC and for convenience in Annex 2.

TSP information URI

This mandatory field specifies the URI(s) where users (e.g. Trusted List relying parties) can obtain CSP specific information. This shall be a sequence of multilingual pointers with English 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. While there must be at least an URI leading to e.g. a web page in English which can be dereferenced in this context, the available documents (CPS, CP's, legal terms, policies, etc.) may not be provided in English but in national language(s) even if English versions would be recommended.

2.2.7 **Listed TSP Services**

This mandatory field 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) and no CSP could be listed in a Trusted List without any listed service.

The certification service entries listed in a Trusted List conform to CD 2009/767/EC specifications [6] amended by Decision 2010/425/EU [7] is made of the following fields:

- The “Service type identifier” (“Sti”), specifying the type of listed certification service (e.g. CA/QC, CA/PKC, TSA).
  This field may be further specified by the “Service information extensions:additionalServiceInformation” (“Sie:aSI”) extension as part of the “Service information extensions” (“Sie”) (e.g. to indicate that the listed CA is actually a Root CA – CA/QC:RootCA-QC; or that an OCSP responder service is meant to support QC with regards to certificate validity status information – OCSP:OCSP-QC).
  It is the combination of the “Sti” and the “Sie:aSI” when this latter is present, that all together specify the type of listed service.;

- The “Service name” (“Sn”);

- The “Service digital identity” (“Sdi”) information identifying a listed service, i.e. the X.509v3 certificate (as a minimum) of a CA issuing QCs;

- The “Service current status” (“Scs”) information for this service entry providing information on:

    - Whether it is a supervised or accredited service, and

    - The supervision/accreditation status itself.

- The “Current status starting date and time” (“Cssdt”) information specifying the date and time on which the current service status became effective

- The optional “Scheme service definition URI” (“Ssdu”) that can be used by the “Scheme operator” to provide additional service-specific information

- The optional “Service supply points” (“Ssp”) information

- The optional “TSP service definition URI” (“Tsdu”) that can be used by the CSP to provide additional service-specific information

- The “Service information extensions” (“Sie”) that may contain three types of extensions:

    - The “additionalServiceInformation” (“Sie:aSI”) extension;
    - The “Qualifications” (“Sie:Q”) extension;
    - The “TakenOverBy” (Sie:TOB”) extension.

  The “additionalServiceInformation” (“Sie:aSI”) extension is used to provide additional information on a service, such as a clarification on the type of service (completing the information provided in “Sti”).

  The “Qualifications” (“Sie:Q”) extension allows, for CA/QC services, to compensate the lack of machine processable information in issued QCs with regards to the QC statement or SSCD support statement, through the 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).

The "TakenOverBy" ("Sie:TOB") extension is present when a service that was formerly under the legal responsibility of a CSP is taken over by another CSP 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.

- A "Service approval history" sequence of information on the previous approval status for each change in the listed service current status which occurred within the historical information period. Each sequence of history information is made of the "Sti", "Sn", "Sdi", "Service previous status", "Previous status starting date and time" and "Sie" fields.

As the retention of historical information about listed services is required under CD 2009/767/EC & 2010/425/EU 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). This means that a CSP must be kept included in the Trusted List even when its only listed service is in such a state, in order to preserve the history, at least for the duration whose value is specified in the "Historical information period" field.

The most critical part of the creation of the Trusted List (TL) is the establishment of the mandatory part of the TL, namely the "List of services" issuing QCs, per CSP, 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).

Insofar as there is no truly interoperable and cross-border profile for the QC, the required information may 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) must therefore take into account the actual 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[18] 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[19]. The use by CSPs issuing QCs of different standards as references, the wide

[18] Refer to ETSI TS 101 862 - Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.
[19] ETSI TS 101 456 - Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

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")[20] fields with information provided in the "Service information extensions" ("Sie") field allows the TL common template specified in [6][7] 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 4 below.

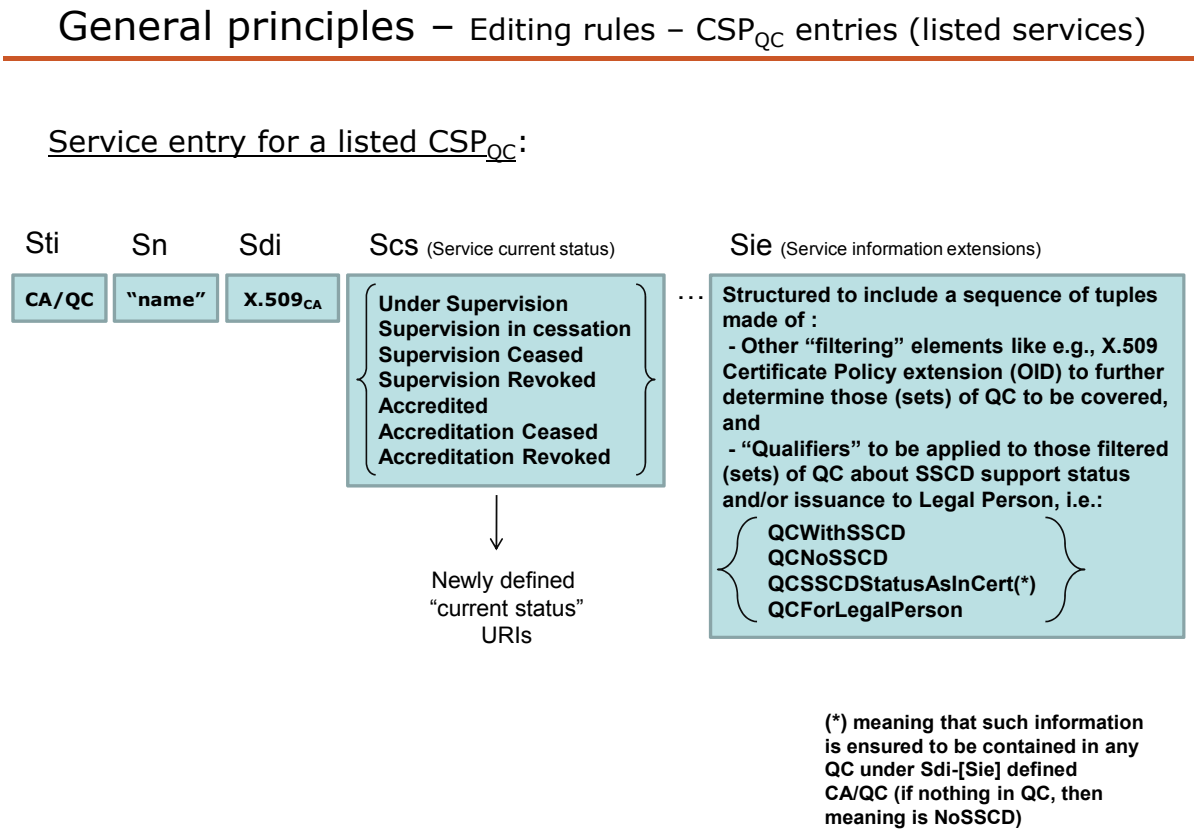


Figure 4: Service entry for a Listed CSP issuing QCs in a Member State Trusted List

Not using the "Sie:Q" extension facility and hence listing a service by just providing the "Sdi" of a (Root) CA (together with the other required service entry fields) 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.

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

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 and not using the “Sie:Q” extension, 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:Q” extension 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).

Editing guidelines for CSP services entries

The only field that is meant to uniquely identify a service is the "Service digital identity" (“Sdi”) (i.e. a "digital identifier unique to the service whose type is defined in the “Service type identifier” field and by which the service can be unambiguously identified" clause 5.5.3). Annex of CD 2009/767/EC further requires a X.509 certificate value as the minimum identifier for such “Sdi”.

The **general default applicable rule** can be stated as follows:

> **"For a X.509 certificate value in the “Service digital identifier”(Sdi) field of a service, there must be only one single entry in a Trusted List per type of service, where the type of a service is determined by the combination of the “Service type information” (Sti) further specified, when present, by the “additionalServiceInformation” (aSI) as part of the “Service information extension” (Sie), i.e. the Sti:Sie/aSI value.**
>
> where examples of Sti:Sie/aSI values are (using shortcomings for applicable URIs as defined in CD 2009/767/EC) are:
>
> - For what is predefined in CD 2009/767/EC
> - CA/QC
> - CA/QC:RootCA-QC
> - CA/PKC
> - CRL
> - CRL:CRL-QC
> - OCSP
> - OCSP:OCSP-QC
> - TSA
>
> - For illustration purposes (and liberally inspired from the French, German or Hungarian situations)
> - CA/PKC:RGS*
> - CA/PKC:RGS**
> - CA/PKC:RGS***
> - TSA:DE-TST-QES (or TSA:DE-QTST)
> - TSA:HU-TST-QES (or TSA:HU-QTST)

In other words, service entries (considering all entries in a Trusted List not only multiple entries for a single TSP) with the same ‘Sti:Sie/additionalServiceInformation’ value must not have the same X.509v3 certificate as “Sdi” (clause 5.5.3).

Changing "Sdi" (e.g. renewal or rekey of a CA certificate) or creating new Sdi, even with identical values for the associated Sti, Sn, and the optional [Sie] fields, means creating a different service than the previous one, thus requiring a new service entry in the Trusted List.

With regards to CSP issuing QCs, as from the above general default rule, 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.

The **associated general editing guidelines** are the following:

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.

Listing Root CA services instead of every root-signed CA service 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.

Similarly for those services (e.g. CRL, OCSP) that are rekeying so often (e.g. every 10 minutes, every hour, every month) that it makes it not practical to reissue a TSL each time, it is expected that those services will be root-signed by a upper level service and it is this service that is expected to be listed in the TSL.

Illustration

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”.

General usage guidelines

The **general usage guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to Technical Specifications [6][7] should be taken into account by TL implementers (i.e. Scheme operators) when editing TL. Those general usage guidelines 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}.

- **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”

Services supporting “CA/QC” services but not part of the “CA/QC” “Sdi”

Provisions stated in Section 2.4 of Annex from CD 2009/767/EC [6] and related to the “*Services supporting “CA/QC” services but not part of the “CA/QC” “Sdi”*could be further clarified as follows[21]:

> *The cases where the keys (and thus the “Sdi”) used by a CA for issuing QCs (“CA/QC”) are different from those keys used to sign CRLs and OCSP responses for those issued QCs, must be covered by listing those CRLs and OCSP 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 “OCSP(Sti):OCSP-QC(Sie/aSI)” or “CRL(Sti):CRL-QC(Sie/aSI)” 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.*

[21] This should be seen as a clarification of the current specifications of CD 2009/767/EC [6] further amended by the forthcoming amendment [7] and should be proposed as an additional amendment to those specifications.

In particular, 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.

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.

2.2.8 Service type identifier

CD 2009/767/EC specifications amended by CD 2010/425/EU related to the Service type identifier clause 5.5.1 could be further clarified as follows[22]:

Service type identifier *(clause 5.5.1)*

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").

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.

When the listed service is related to a Time Stamping Authority (TSA) service which is issuing Time Stamp Tokens (TST) that can be used in the verification process of a QES, it SHALL be made use of the following combination of URIs:

- *"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 associated with the description below:

  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.

As a general principle, for a X.509 certificate value in the "Service digital identifier" (clause 5.5.3) field of a service, there must be only one single entry in a Trusted List per type of service, where the type of a service is determined by the combination of the "Service type information" (clause 5.5.1) further specified, when present, by the

[22] This should be seen as a clarification of the current specifications of CD 2009/767/EC [6] further amended by the forthcoming amendment [7] and should be proposed as an additional amendment to those specifications.

"additionalServiceInformation" (clause 5.8.2) as part of the "Service information extension" (clause 5.5.9), i.e. the "Sti:Sie/aSI" value.

With regards to CSP issuing QCs, as from the above general 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 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[23]. In addition, when using such an authorized exception to the general principle, Member States MUST provide the necessary documentation to facilitate the certification path building and verification.

When the listed service is related to a Root CA service from which a certification path can be established down to a CA service issuing QCs, it SHALL be made use of the following combination of URIs:

- *"Service type identifier" (clause 5.5.1) value:*
  http://uri.etsi.org/TrstSvc/Svctype/CA/QC

  combined with the following "Service information extension" (clause 5.5.9) additionalServiceInformation extension (clause 5.8.2) value associated with the description below:

  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.

TSPs like OCSP responders and CRL Issuers that are part of CSP_{QC} certification services and either subject to the use of separate key pairs to respectively sign OCSP responses and CRLs or for which the related access information is not present in the AIA field of end certificates, MUST be listed as well in the TSL implementation of the Trusted List by using the following combination of URIs, respectively:

- *"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 associated with the description below:
  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

[23] 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.

combined with the following "Service information extension" (clause 5.5.9) additionalServiceInformation extension (clause 5.8.2) value associated with the description below:
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.

2.2.9 **Service digital identity**

As a general default principle, the digital identifier (i.e. as a minimum the related X.509v3 certificate that the CSP uses for providing the service whose type is specified by the "Service type identifier" (clause 5.5.1) and potentially further specified by the "Service information extension" (clause 5.5.9) additionalServiceInformation extension (clause 5.8.2) value) shall not be present more than once in the Trusted List for this "Sti:Sie/aSI" type value. This means that there shall be one entry per single X.509v3 certificate for a specific certification service type under the listed certification services in the Trusted List. Conversely, one single X.509v3 certificate SHALL be used in a single service entry as the "Sdi" value.

The sole case for which an "Sdi" X.509v3 certificate value may appear in several entries is when a single X.509v3 certificate is used for 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 scheme and 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.

When the same certification service is listed in different Trusted Lists (e.g. a certification service issuing QCs being supervised in the Member State where it is established and accredited in another Member State), the entry used in the TL where it is not established shall use the same values for the "Sti:Sie/aSI", "Sn", "Sdi" X.509v3 certificate, and "Sie:Q" fields without prejudice of adding any relevant and consistent information in the service entry.

When a listed service is changing of "Sdi" value (e.g. due to renewal or rekey of a CA certificate) or is creating a new Sdi, even with identical values for the associated "Sti", "Sn", and the optional "Sie" fields, this requires for creating a different service than the previous one, thus requiring a new service entry in the Trusted List.

2.2.10 **Status determination approach and status information flow**

The services listed in the Trusted List have their status determined by or on behalf of the Scheme Operator[24] 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 of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 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.

[24] i.e. either by a Supervisory Body or an Accreditation Body , when applicable.

One single Trusted List must be established and maintained per Member State to indicate the supervision and/or accreditation status of those certification services from those CSPs, issuing QCs or not, that are accordingly supervised/accredited by the Member State.

The fact that a service is currently either supervised or accredited is part of its current status. Figure 5 below describes the flow, for one single certification service whether issuing qualified certificates or not, between possible supervision/accreditation statuses.

Throughout its lifetime, the same certification service can be "ongoing", "in cessation", "ceased", or even "revoked" and may move from a supervision status to an accreditation status and vice versa. E.g. a certification service provider established in a Member State that provides a certification service issuing qualified certificates 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 whatever business and/or economic reasons.

Expected supervision/accreditation status flow for a single CSP service

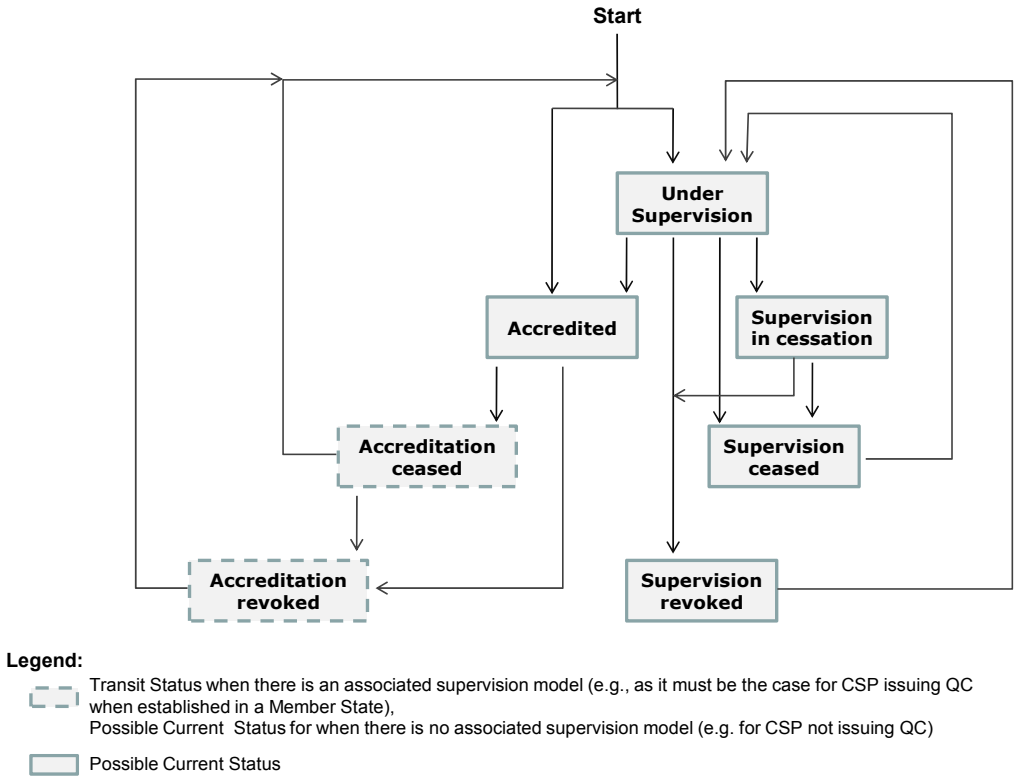


Figure 5

The status value of a certification service when listed in a Trusted List can have any of the depicted status values as "current status value". Those values shall be interpreted as follows[25]:

[25] For exact definition of those status values, please refer to CD 2009/767/EC and in particular to specifications of clause 5.5.4 ("Service current status") or to Annex 2 of the present report.

- ***Under Supervision***: The service identified in the entry of the Trusted List and provided by the associated identified Certification Service Provider (CSP) is currently under supervision, for compliance with the provisions laid down in Directive 1999/93/EC, by the Member State owner of the Trusted List and in which the CSP is established.

- ***Supervision of Service in Cessation***: The service identified in the entry of the Trusted List and provided by the associated identified Certification Service Provider (CSP) is currently in a cessation phase but still supervised until supervision is ceased or revoked. In the event a different legal person than the associated CSP identified as in cessation 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 the service entry.

- ***Supervision Ceased***: The validity of the supervision assessment has lapsed without the service identified in the entry of the Trusted List 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 owner of the Trusted List and 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.

  It should be noted that 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 Trusted List, 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 owner of the Trusted List and the service identified in the associated entry and provided by the associated identified CSP[26] is found to be in compliance with the provisions laid down in Directive 1999/93/EC.

When used in the context of a CSP issuing QCs that is established in the Member State owner of the Trusted List, 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 5. When used in the context of a CSP not issuing QCs when there is only an associated "voluntary

[26] 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).

accreditation" scheme with no associated supervision scheme or in the context of a CSP issuing QCs where the CSP is not established in the Member State owner of the Trusted List (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 the associated entry of the Trusted List being re-assessed.

- ***Accreditation Revoked***: Having been previously found to be in conformance with the scheme criteria, the service identified in the associated entry of the Trusted List and provided by the associated Certification Service Provider (CSP) and potentially the CSP itself have failed to continue to comply with the provisions laid down in Directive 1999/93/EC.

Any Member State must establish an appropriate supervision system for certification services established in its territory and issuing qualified certificates, but it may also establish:

- one or several supervision systems for any other type of certification service ancillary to electronic signatures,
- one or several 'voluntary accreditation" systems for any type of certification service including issuing of qualified certificates.

For that purpose, 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 Directive 1999/93/EC) 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.

The type of certification service will determine which type of supervision/accreditation system will apply in the context of the Member State in which it is established or applied for.

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.) when listing such certifications services in a Trusted List. The identifier of the type of service that is listed in an entry of the Trusted List shall be used to distinguish between applicable supervision/accreditation systems (e.g. CA issuing QC, CA issuing non-qualified certificates, other types of CSPs like Time Stamping Authorities, etc.).

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 for that purpose a specific extension of the service entry namely the "additionalServiceInformation" extension as part of the "Service information extension" field.

2.2.11 **Current status starting date and time**

The date and time on which the current supervision/accreditation ("approval") status became effective is provided per listed service entry as well as the whole related historical information according to a retention period (this latter being also expressed in the Trusted List).

2.2.12 **Scheme service definition URI**

The Scheme Operator has the possibility to use this field to provide relying parties with service-specific information through the means of a sequence of URIs leading to information describing such specific information about the associated listed service.

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;

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 an "additionalServiceInformation" extension as part of the "Service information extension" field.

2.2.13 **Optional service information given by the TSP**

The "Service supply points" and "TSP service definition URI" fields can be used to provide information on respectively where relying parties can access the service and where they can obtain service-specific information provided by the TSP.

2.2.14 **Service information extension**

This field while optional is however used in two specific circumstances.

- It is mandatorily used when the information provided in the "Service digital identity" 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 it is (claimed to be) a QC and whether or not the QC is supported by an SSCD[27].

- It may be used as an option to provide additional information on a service in order, e.g., to indicate some nationally defined specific qualification and/or legal status for a supervised/accredited Trust Service Token provisioning service. See clause 5.8.2 in Annex of CD 2009/767/EC [6] [7] for further details.

For those QC for which there is a lack, in their content, of machine-processable information with regards to their claimed status as QC and/or with regards to the fact that the private key associated with the public key in the certificate resides within a Secure Signature Creation Device, and/or the fact that the QC is issued to a legal person, this "Service information extensions" ("Sie") information field shall be used and structured, according to the "Qualifications" extension ("Sie:Q"). This "Sie:Q" extension 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

[27] See section 2.2 of the present document.

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. In this case when there is no machine-processable information about such an SSCD support in the content of a QC, then it must be considered that the private key associated with the public key in the certificate does not reside within a Secure Signature Creation Device (hence an AdES supported by such a certificate cannot be considered as a QES);

  AND/OR

- to indicate issuance to Legal Person:
  - “QCForLegalPerson” qualifier value meaning “Certificate issued to a Legal Person”

As an example, and as extracted from the Belgian TSL xml implementation of the Belgian Trusted List, the following xml encoding of the “Sie:Q” extension has the meaning described below:

```
- <tsl:ServiceInformationExtensions>
  - <tsl:Extension Critical="true">
      - <ecc:Qualifications>
        - <ecc:QualificationElement>

            - <ecc:Qualifiers>
              <ecc:Qualifier uri="http://uri.etsi.org/TrstSvc/eSigDir-1999-
                93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert" />
              </ecc:Qualifiers>
            -
              <ecc:CriteriaList assert="atLeastOne">
                  - <ecc:PolicySet>

                    - <ecc:PolicyIdentifier>
                      <xades:Identifier>2.16.56.1.1.1.2.1</xades:Identifier>

                        <xades:Description>urn:be:qc:natural:citizen</xade
                        s:Description>
                      </ecc:PolicyIdentifier>

                    - <ecc:PolicyIdentifier>
                      <xades:Identifier>2.16.56.1.1.1.7.1</xades:Identifier>

                        <xades:Description>urn:be:qc:natural:foreigner</x
                        ades:Description>
                      </ecc:PolicyIdentifier>
```

```
                    </ecc:PolicySet>
                  </ecc:CriteriaList>
                </ecc:QualificationElement>
              </ecc:Qualifications>

- <tsl:AdditionalServiceInformation>
  <tsl:URI xml:lang="en">http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-
    TrustedList/SvcInfoExt/RootCA-QC</tsl:URI>
    </tsl:AdditionalServiceInformation>
    </tsl:Extension>
  </tsl:ServiceInformationExtensions>
```

Meaning: The information present in the above "Sie" field (note the presence of both an "Sie:Q" extension and an "Sie:aSI" extension) is a means to express the fact that within the hierarchy of CAs under the "Sdi" defined X.509v3 Root-CA certificate (see the "Sie:aSi" extension), it has been validated by the Belgian Supervisory Body (as claimed by and under the responsibility of the related CSP) that all issued certificates do contain relevant machine-processable information with regards to the claimed QC status and the claimed SSCD support[28] except those certificates that contain at least one of the above specified OIDs (respectively 2.16.56.1.1.1.2.1 and 2.16.56.1.1.1.7.1) for which there is a lack of information with regards to the SSCD support claim. This lack of information is compensated by the "**QCSSCDStatusAsInCert**" meaning that for those certificates with a Policy identifier 2.16.56.1.1.1.2.1 or 2.16.56.1.1.1.7.1, a lack of use of machine-processable with regards to the claimed SSCD support must be strictly interpreted as the private key associated with the public key in those certificates **does not** reside within a Secure Signature Creation Device.

2.2.15 Service approval history

In the context of the Trusted List specifications [6] [7], the Trusted Lists must retain historical information at least for the last 3653 days.

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 must be left empty. Otherwise, for each change in TSP service current status which occurred within the historical information period, information on the previous approval status must 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). This must be a sequence of history information entries each of them made of the following fields:

- "Service type identifier" (clause 5.6.1 with a value identical as the one stated in clause 5.5.1 with regards to the listed service entry),
- "Service name" (clause 5.6.2 with a value potentially different form the one in clause 5.5.2 as a change of name may be a (side) effect of one of the circumstances requiring a new status,
- "Service digital identity" (clause 5.6.3 specifying at least one representation of the digital identifier i.e. the X.509v3 certificate) used in the "Sdi" clause 5.5.3 of the related listed service entry,

[28] Or more correctly that to the fact that the private key associated with the public key in the certificate resides within a Secure Signature Creation Device.

- "Service previous status" (clause 5.6.4 specifying the previous status of the service),
- "Previous status starting date and time" (clause 5.6.5 specifying the date and time on which the previous status in question became effective),
- And the optional "Service information extension" (clause 5.6.6 that may be used to provide specific service related information).

With regards to the "Sdi" clause 5.6.3 in the historical information, we can note the following:

- 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/aSI' value[29]. 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 be present;
    - Must relate to the same X.509v3 certificate value;
    - May not be the full X.509 certificate as it is required in the main part of the service entry (i.e. clause 5.5.3) but it can simply be the SubjectKeyIdentifier (SKI), the DistinguishedName (DN) or another representation of the "Sdi" provided in the main part of the service entry.

      The size of a Trusted List for which some services do have a (long) historical information may be considerably reduced when the full X.509v3 certificate is not duplicated at each historical information but represented by another representation of the exact same certificate.
- 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.
- Consequently and for the sake of clarity, there cannot be a situation in which an "historical information Sdi" (clause 5.6.3) is specifying a digital certificate:
    - that is different from the "Sdi" certificate value in the service entry "Sdi" field (clause 5.5.3), or
    - that is issued to another legal entity than the TSP to which the corresponding listed service is associated. This is also applicable for the "Sdi" certificate value in the service entry "Sdi" field (clause 5.5.3).

2.3 Signing Trusted Lists

As per the amendment [7] of CD 2009/767/EC [6], Member States must:

- establish and publish both a human readable and a machine processable form of the Trusted List;
- sign electronically the machine processable form of their Trusted List; and

[29] See "Editing guidelines for CSP services entries" in section 2.2.7 of the present report.

- should sign the human readable and when not signing it, they must, as a minimum, publish the human readable form of the Trusted List through a secure channel in order to ensure its authenticity and integrity

The format of the Human readable form of the Trusted List signature should be PAdES part 3 (ETSI TS 102 778-3[30]) but may be PAdES part 2 (ETSI TS 102 778-2[31]) 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 (an XML implementation complying with the specifications stated in Annexes B and C of ETSI TS 102 231) must be signed using a XAdES BES or EPES format as defined by ETSI TS 101 903 specifications for XML implementations. Such electronic signature implementation must meet requirements as stated in Annex B of ETSI TS 102 231.[32] Additional general requirements regarding this signature are stated in the "Scheme identification" (clause 5.7.2), "Signature algorithm identifier" (clause 5.7.3) and Signature value (clause 5.7.4) sections of the amended version [7] of CD 2009/767/EC [6].

2.4 Trusted List Trust Model

As per the amendment [7] of CD 2009/767/EC [6], a national Trusted List is a signed document (machine-processable version and potentially the human readable version) or at least a document which is protected by a public key certificate based secure channel (e.g. TLS or SSL based sessions).

To verify the signature of the Trusted List or the public key certificate used to implement the certificate channel, relying parties need to be able to access the applicable public key. Since the scheme on the basis of which issuing Trusted List is effectively positioned "above" the TSPs approved by that scheme, the authenticity of the public key cannot be verified solely on the basis of its certification by any TSP inside or outside the scheme. Providing the scheme's public key is therefore a problem very similar to providing the public key of a CA service and in this context, the amendment [7] of CD 2009/767/EC [6] establishes a Trust Model based on:

- The notification by Member States to the Commission of 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;

[30] 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.

[31] 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.

[32] 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.

(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).

From these notifications, the Commission is making available to all Member States, through a secure channel to an authenticated web server, the above referred information as notified by Member States under the form of a Compiled List of links towards the Member States' national Trusted Lists.

With specifications in compliance with ETSI TS 102 231 [5], the centrally available Compiled List (the European Commission list of the locations where the Trusted Lists are published as notified by Member States) is available on a secure web-site both in a human readable format (TSL/SSL protected)[33] and in a signed machine processable format[34].

Rather than having each Member State publishing the certificate used by the Scheme Operator to sign its national Trusted List in a national official journal or alike, which could be difficult for relying parties to access or to validate, all Member States use the same formal notification process established between Member States and the European Commission with regards to the above referred information. Despite the disclaimer stated by the European Commission[35], this notification process, the notified information, and the protection measures given to the Compiled List provide a sufficient guarantee of Trust to the information contained in such a central list and to the .

The certificates used by the European Commission Scheme Operator when respectively signing the machine-processable version and securing the human readable version of the Compiled List are published of the locations where the Trusted Lists are published as notified by Member States and to the integrity and authenticity of the public key certificates to be used to authenticate the national Trusted Lists.

With regards to the type of public key certificate, their security and quality, self-signed keys established according to the state of the art, by, or on behalf of, national Scheme Operators may prove to be a suitable solution. Commercially available signing key pairs and related public-key certificates from a certification service provider whose issuing certification service is listed in the Trusted List to be signed with such a certificate, or listed in another Trusted List or not listed in any Trusted List may also prove to be suitable. In all cases it would be recommended to use state-of-the-art quality and security key management practices that are at least equivalent to the services listed in the Trusted List.

Nevertheless it is not the trust model inherited from the potential commercial or not PKI hierarchy issuing the Scheme Operator certificate that will bring the authenticity and trust to this certificate but rather its notification process to the Commission and its inclusion and publication in the European Commission Compiled List.

2.5 Specific cases

November 2009, a Trusted List implementation workshop and Trusted Lists testing facilities were set up jointly by the European Commission and ETSI. The main objective of these so-called TSL PlugTests was twofold and can be split into the following two interrelated Plans:

[33] https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf
[34] https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml
[35] See https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl.html#en

- **1. TSL Lifecycle Management Tests:** Allowing each Member State to test the publishing and lifecycle management of the TSL implementation of their Trusted List (e.g. creation of the first version of the TSL, update of the existing entries with regards to supervision/accreditation status, inclusion of new services to be listed). The associated Test Plan included the conformity check of Member States' TSLs against the Trusted List Technical Specifications as set out in CD 2099/767/EC [6].

- **2. TSL Interoperability Tests:** The purpose of this second Test Plan was to validate the simulated use of the Trusted Lists TSL implementations in cross-border use (validation) of qualified electronic signatures and advanced signatures based on qualified certificates. Those tests were conducted in parallel with the lifecycle management tests of the TSL to validate the effects of such tests in the context of the validation of electronic signatures.

Specific ETSI support and ETSI TSL testing facilities are still available to Member States for further testing conformity of their national Trusted List TSL implementations, in particular the ETSI TSL Conformance Checker[36].

One of the deliverables of those late 2009 TSL PlugTests, namely the "TSL contents for the TSL lifecycle test cases" [9], aimed to serve as a starting point Tutorial for building up a common view on how a Trusted List TSL implementation would change its contents when listed services, listed CSPs, or Scheme Operator details suffer specific changes.

The next sub-sections will highlight some specific changes or situations that may occur when maintaining a Trusted List and provide explanations on how these changes should be addressed.

2.5.1 Listed certification service taken over by another CSP

Next paragraphs describe best practices to cessation of listed CSP services whatever the reasons might be, e.g. the consequence of TSP merges or concentrations:

> A TSP wishes to enter a process of cessation of either all of its services, or only one or several services from those services that are either supervised or accredited according to the current service(s) status as listed in the TL of the Member State in which it is established or accredited.
>
> **Option 1**: The service(s) to be ceased from the former TSP are transferred to another recovering TSP without the need to revoke active issued certificates. In this case, the recovering TSP will only ensure the lifecycle management of the existing issued certificates (e.g., OCSP, CRL certificate validity status services).
>
> **Option 2**: The active certificates issued by the service(s) to be ceased from the former TSP are all revoked (note that this process should be completed by the revocation of all related CSP_{QC} certificates operated by the former TSP in the context of the services to be ceased). In this case, the Member State in which the former TSP issuing QCs is(was) established or accredited (e.g., the Supervisory Body, the Accreditation Body or any other designated Body) must ensure that CRLs, certificates and related subscriber information will be recorded electronically for the purpose of providing evidence information of certification in legal proceedings. This mandatory recording can be operated by a Member State Body, a designed third party, or in the

[36] See on http://xades-portal.etsi.org/pub/aboutTSL.shtml.

event the former TSP services activities are still transferred to another recovering TSP, to this recovering TSP[37].

In the context of both options, when the former TSP services activities are transferred to another recovering TSP, several sub-cases (sub-options) are possible and can be described as follows:

- **Option 1/2.A**: No new certificates will be issued by the recovering TSP on the basis of the CSP_{QC} private key pair(s) referred to from the current "Sdi" value in the service(s) entry(ies) related to the service(s) to be ceased in the Member State TL. When recovering the services from the former TSP, and wishing to exploit those recovered services, the recovering TSP shall generate new CSP_{QC} key pair(s) and associated CSP_{QC} certificate(s) for the purpose of issuing new QC from the recovered services or infrastructure. Since CD 2009/767/EC technical specifications (hereafter referred to as "The Specifications") require the use of a X.509v3 certificate as primary value for an "Sdi", this new CSP_{QC} key generation and CSP_{QC} certificate issuing process will lead to new "Sdi"'s to identify those new services from the recovering TSP and hence new entries in the TL as part of the listed services from the recovering CSP.

- **Option 1/2.B**: New certificates will be issued by the recovering TSP on the basis of the same CA/QC private key pair(s) referred to from the current "Sdi" value in the service(s) entry(ies) related to the service(s) to be ceased in the Member State TL[38]. In this context it SHALL not be allowed to the recovering TSP to use the same CA/QC certificates as those used by the former TSP since those former QCA certificates are likely to refer to the former TSP organization has the legal entity to be linked to the CA/QC as "Issuer" of the certificates. Consequently, in this context the recovering TSP must be required to create new certificate(s) for the CA/QC(s) whose private key pair(s) are referred to from the current "Sdi" value in the service(s) entry(ies) related to the service(s) to be ceased in the Member State TL. Since the "Technical Specifications" require the use of a X.509v3 certificate as primary value for an "Sdi", this new CA/QC certificate issuing process will lead to new "Sdi"'s, and hence new service entry(ies), to identify those new services from the recovering TSP.

- **Option 1/2.C**: New certificates will be issued by the recovering TSP on the basis of new CA/QC private key pair(s) than those referred to from the current "Sdi" value in the service(s) entry(ies) related to the service(s) to be ceased in the Member State TL. Since the "Technical Specifications" require the use of a X.509v3 certificate as primary value for an "Sdi", this new CA/QC key pair(s) generation and CA/QC certificate issuing process will lead to new "Sdi"'s, and hence new entry(ies), to identify those new services from the recovering TSP.

From the possible options related to the "TSP cessation case" described here above, it can be summarized that, in the event the recovered services (to be) operated by the recovering

[37] It may however be the case that services from the former TSP issuing QCs are still transferred to a recovering TSP while the above mentioned mandatory recording obligation is operated by another party than the recovering TSP.

[38] Depending on what the "Sdi" is actually referring to, this may refer to a large number of issuing CA/QC key pairs each issuing end-entity QCs.

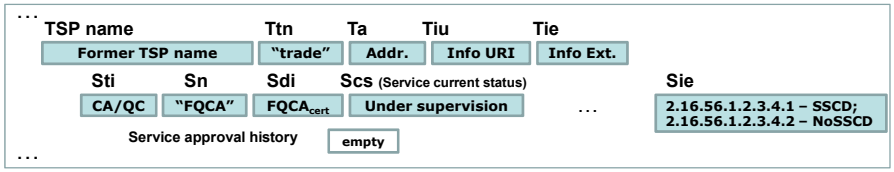
TSP are still assessed[39] by the Member State Supervisory or Accreditation Body, such a cessation will always lead to the following TL update as illustrated below:

- Coming from a "Under Supervision" status, the new status shall be "Supervision of service in cessation" while the clause 5.5.6 can be used by the Scheme Operator, when applicable, to indicate the identification information of the recovering TSP, and whatever appropriate information about this recovering process (see Figure 6);

- Coming from an "Accredited" status, the new status shall be "Supervision of Service in Cessation", through the successive statuses of "Accreditation Ceased" (or alternatively "Accreditation revoked" when applicable), and "Under Supervision" as illustrated in the new "service approval history" in Figure 7 and according to the expected status flow illustrated in Figure 5. "TakenOverBy" extension and clause 5.5.6 can be used by the Scheme Operator, when applicable, to indicate the identification information of the recovering TSP, and whatever appropriate information about this recovering process.

QTSP services cessation from "Under Supervision" status

Former entry into TL regarding the TSP in cessation, i.e.,



becomes, once it is acted by the Supervision Body to be in cessation,

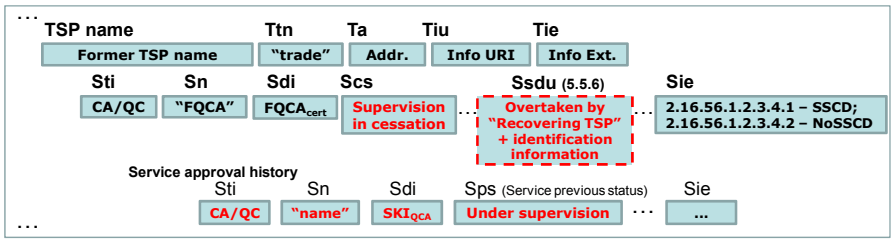
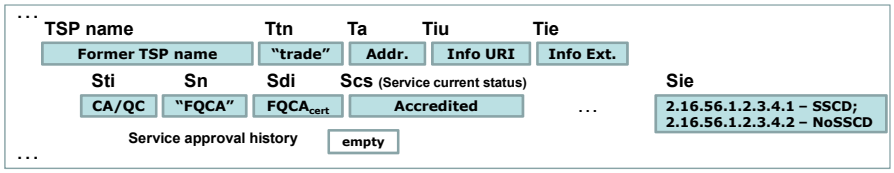


Figure 6

[39] i.e., "controlled" in the event of a supervision, or "audited" in the event of an accreditation.

Former entry into TL regarding the TSP in cessation, i.e.,



becomes, once it is acted by the Supervision Body to be in cessation,

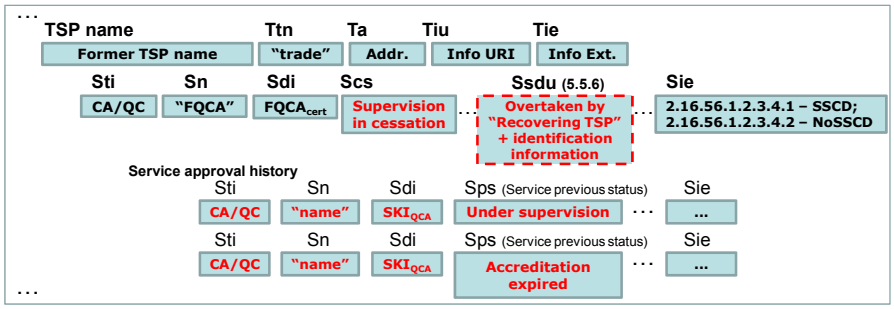


Figure 7

In the event, the recovering TSP passes the supervision or accreditation process for the new services built upon the recovered services from the former TSP, this will always result as described here above in the creation of one (or several) new entry(ies) for such a (to be) listed TSP organisation with "Sdi" value(s) that will be different from the one(s) associated to the former TSP.

As a summary, the following rules apply when a listed service is taken over by another TSP:

- The service entry is never duplicated (except specific case allowed by [6][7] for QC discrimination versus PKC) or moved in the TSL and the service remains listed under its original CSP;
- The verification process takes into account only the status of the related instance of the service present in the TSL, identified by its Service Digital Identity;
- The service status should move to "supervision in cessation" but might also remain unchanged ("accredited" or "under supervision") and it is the responsibility of the Scheme Operator to maintain accurate the trust relationship of the service;
- If a takeover happened, the Legal entity recovering and managing the service some information has to be published and pointed by the URI using TS 102 231 clause 5.5.6 and/or by making use of the "TakenOverBy" extension [7], with an URI providing the same information as in previous point and an optional identification of the taking over CSP (e.g. Scheme name, TSP name and Scheme territory)
- When processing this, the information provided about the taking over CSP is provided for information display only in order to provide some processing context information to the relying parties.

2.5.2 Clarifications of the meaning for “Supervision of Service in Cessation” and “Supervision Ceased” status values

Usually 'in cessation' is triggered by the CSP. A CSP may notify to the Scheme Operator the fact that some of its listed services are currently being driven into cessation. But still any service in cessation is being supervised, until the service is actually ceased (or revoked).
The official description is the following (Decision 2010/425/EU, Annex §1.(k) [7] amending Decision 2009/767/EC [6]):

> ***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.’*

'Supervision Ceased' is reached after 'supervision in cessation', although it may also be reached from 'undersupervision'. The service is stopped. The official description is the following (Decision 2009/767/EC, page 41 OJ L299):

> ***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' is reached after not having passed the supervision process. The official description is the following (Decision 2009/767/EC, page 41 OJ L299):

> ***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.*

2.5.3 Changing the name of a listed service

Trusted Lists specifications [6] [7] specifies that this element "SHALL specify the name under which the TSP provides the service identified in clause 5.5.1". A change of service name is however not likely to occur for the sake of changing name but be motivated by more fundamental reasons that would have a effect on the changes required. Depending on these reasons, the nature of the required changes will be different and must remain consistent with the actual situation of the listed service as supervised or accredited by the Supervisory or Accreditation Body in charge. Typical reasons for service name change are listed below without the pretention to be exhaustive:

- Changes done under the umbrella of the same TSP:
    - ***The name of the service changes as the “Sdi” value for this service changes***: Section 5.5.3 of CD 2009/767/EC’s annex [6] [7] specifies that the DigitalIdentity element "SHALL specify at least one representation of a digital identifier unique to the service specified in clause 5.5.1". If the name of the service changes is accompanied by a change of “Sdi” value, even if it is

provided by the same TSP, the following changes shall appear in the TSL: a new service entry must be added in the list of services provided by the corresponding TSP, with the new digital identity.

Any change to the status of the former service (Service entry having the former “Sn” name value and former “Sdi” value”) must be reflected accordingly. E.g. when the former named service is stopped by the TSP, then the status of this service should be changed accordingly (i.e. from “Under supervision” to “Supervision in Cessation”, or “Under supervision” to “Supervision Ceased”, or “Supervision in Cessation” to “Supervision Ceased”, or “Under supervision” to “Supervision Revoked”, or one valid flow from the “Accredited” status to a another status reflecting the actual status of the former named service).

- ***The name of the service changes for pure commercial reason but no change is required in the associated “Sdi” value***: Since the historical information associated to a listed service is meant to be associated to the service approval history, reflecting a Service name change without any change in the service approval status would have as a consequence that the service name history would not be retained.

- Change done due to the service takeover by another TSP: see section 2.5.1 for further guidance.

2.5.4 **Name change of a listed TSP**

Trusted Lists specifications [6] [7] specifies that, CSP name, clause 5.4.1 "SHALL specify the name of the legal entity responsible for the CSP's services that are or were supervised or accredited under the scheme". Thus changing CSP name means a change of responsible legal entity. It should be kept in mind that the unique identifier for a service is the service digital certificate (not the public key but the certificate).

Reasons for moving services from one legal entity to another can be:

- The CSP did not mean to really stop CSP commercial services as such but needs to change legal name because of reasons external to the provision of such services (merging, acquisition, changing legal form of company, etc.)
- The CSP decides to stop those commercial services and transfer them to another company
- The CSP did not decide anything but was forced to stop its services
  - because of bankruptcy
  - because of it failed supervision assessment, could not recover and its commercial services are taken over by another company
  - etc

Consequently such a change forces the new legal entity responsible for listed certification services to have new DigitalId (i.e. new certificate (*)). The entry corresponding to the CSP under its former name would see its services (being taken over) going to a status reflecting the exact situation:

- "Supervision in cessation" when the service(s) is (are) maintained as such but under the responsibility of another company as mentioned in the “Sie:TOB” extension (clause L.3.2) and optionally in "Ssdu" (clause 5.5.6). For CA/QC, CA/QC:Root-CA,

CA/PKC, CA/PKC:xxxx, TSA, TSA:TSS-QC, TSA:xxx type services, it is likely that those services will not issue any more certificates but would continue to provide certificate status validity services (e.g. OCSP, CRL). For OCSP, CRL, OCSP:OCSP-QC, CRL:CRL-QC type services, it is likely that those services will either continue their services (but under a "Supervision in cessation" status and under the responsibility of the taking over CSP (clause 5.5.6) or being ceased.

- "Supervision ceased" when the service(s) is (are) not maintained as such but moved under the responsibility of another company as mentioned the “Sie:TOB” extension (clause L.3.2) and optionally in "Ssdu" (clause 5.5.6), e.g. for archiving obligations.
- "Supervision revoked" when those services are forced by the Supervisory Body to that status and optionally the remaining obligations are transferred to another company.

2.5.5 Expiration of a listed service digital certificate

There is no strict rule mandating the change of supervision/accreditation service current status from “Under Supervision” to “Supervision Ceased” when a CA/QC (or another listed certification service) certificate expires. It is up to the Supervisory Body or Accreditation Body to decide but it is likely that those services will remain under supervision even after expiration of the certificate. The Trusted List should reflect the decision of the Body in charge.

2.5.6 The specific case of a National Root-CA certification service used in the context of CA/QC services accreditation

In some Member States, there exists a specific national Root-CA PKI hierarchy and infrastructure that is mainly, or sometimes exclusively, used to root-sign CA/QC or CA/QC:RootCA-QC when those certification services pass the applicable voluntary accreditation. It may be that such accredited CA’s have a certificate issued by the national Root-CA without having a corresponding self-signed CA certificate. The question is : must this national Root-CA certification service be listed in the Trusted List instead or in addition to the root-signed CA/QC services?

Listing the sole national root is not permitted as implicitly ruled by [6][7] and as per the definition of the Trusted List (TL). The Trusted List aims to provide information on the supervision and/or accreditation status of those services from CSPs that are supervised and/or accredited by a Member State (the one in which the CSP is established or accredited) for compliance with the relevant provisions laid down in Directive 1999/93/EC. The TL must list all supervised (and potentially accredited) services issuing QCs from CSPs established in the Member State that are supervised (and potentially accredited) under the respective CSP entries (TSP name, etc.) and those CSPs issuing QCs that are not established in the Member State but accredited. The TL, on a voluntary basis, can list all supervised (and potentially accredited) services not issuing QCs from CSPs established in the Member State that are supervised (and potentially accredited) under the respective CSP entries (TSP name, etc.) and those CSPs that are not established in the Member State but accredited. Trusted Lists are organized per supervised / accredited CSP (meaning legal entity being responsible for the provision of the listed services), listing the sole national Root-CA that is root-signing such CSPs when they are accredited and not the accredited CSP and their accredited services is not permitted.

When the national root-accreditation-CA is not issuing QCs itself, it is not as such supervised for issuing QCs. Listing such a service in the TL would require and mean that there is a specific “supervision or accreditation” approval scheme used by the Member State to list such a CA/PKC service under some governmental TSP name entry in the TL. **If and only if**

this is the case, Member State can list such a national root-accreditation-CA in the Trusted List.

This means that the national (accreditation) Root-CA which does not issue qualified certificates directly but is used for the technical accreditation identification must not be included in TSL **unless**, as described above, there is a specific "approval scheme" that justifies this entry (CA/PKC) in the TL.

This means as well that such national (accreditation) Root CA is not required to be included and must not be included together with accredited CAs **unless**, as described above, there is a specific "approval scheme" that justifies this entry (CA/PKC) in the TL.

Listing the CA certificate in a Trusted List maintained by an accreditation/supervision body of a member state is enough to establish trust, regardless of whether we can track the certificate path down (or up) to such the national Root-CA". The TL comes as a secondary source of information in the context of validating a QES or $AdES_{QC}$. If in the verification process it is needed, according to some applicable signature validation policy, to further check that a specific certification path is valid (e.g. leading up to a national Root-CA), this is outside the scope of the TL.

In the specific case in which accredited CA's have a certificate issued by the national Root-CA without having a corresponding self-signed CA certificate, from the QES or $AdES_{QC}$ signer's QC, one should directly find the certificate from the issuer of this signer's QC in the TL. In the event where the corresponding CA/QC service entry is actually a Root CA (the signer's QC is issued by a technical CA/QC that is root-signed not by a national-root-accreditation CA but a TSP root CA – in which case the entry type in the TL would then be CA/QC:RootCA-QC (Sdi:Sie))[40], then in order to facilitate certification path building and validation, CD 2009/767/EC requires that Member State "must provide the necessary documentation to facilitate the certification path building and verification". But this is a totally different context than the root-accreditation-CA one.

2.6 Further technical aspects related to Trusted Lists implementation

Other specific requirements regarding technical aspects of Trusted List implementation, not explicitly covered by CD 2009/767/EC [6] as amended by CD 2010/425/EU [7] must be found in ETSI TS 102 231 v3.1.2 [5], in particular with regards to:

- publication of the TSL implementations (machine-processable and human readable) of the Trusted List (section 6.1 [5]),
- TSL distribution points (section 6.3 [5]),
- XML files to be used when implementing TSL implementation of Trusted Lists (Annex C [5]).

[40] This is for example the case when a CSP has so many subordinate CA really issuing QCs under a Root-CA that it would be difficult to list them all (e.g. BE case for eID QCs) and easier to list the TSP Root-CA instead.

3 Future improvements for Trusted Lists

The present section provides some proposals for the next review of CD 2009/767/EC [6] as updated by Decision 2010/425/EU [7], i.e. for a potential third version of CD 2009/767/EC.[41]

3.1 Service type identifier (Clause 5.5.1)

Specifications related to the Service type identifier clause 5.5.1 could be further clarified as proposed in section 2.2.8 of the present report.

3.2 Services supporting "CA/QC" services but not part of the "CA/QC" "Sdi"

Provisions stated in Section 2.4 of Annex from CD 2009/767/EC [6] and related to the "*Services supporting "CA/QC" services but not part of the "CA/QC" "Sdi"*"could be further clarified as proposed in section 2.2.7 of the present report on page 25.

3.3 TSL Signing entity

The fourth paragraph following the section title "Scheme operator name (clause 5.3.4)" is replaced by the following:

> "The named Scheme Operator (clause 5.3.4) SHALL be the entity who signs the TSL."

The first sentence of the first paragraph of the section entitled "Signed TSL" is replaced by the following:

> "The human readable TSL implementation of the Trusted List, established under the present specifications and in particular Chapter IV, SHOULD be signed. When signed, the signer SHALL be the entity identified by the "Scheme operator name" (clause 5.3.4) to ensure its authenticity and integrity[42]."

3.4 Signed TSL

The section entitled "Scheme identification (clause 5.7.2)", the section entitled "Signature algorithm identifier (clause 5.7.3), and the section entitled "Signature value (clause 5.7.4)" are respectively replaced by the following:

> **"Scheme identification** (clause 5.7.2)
>
> This field is REQUIRED and SHALL comply with specifications in clause 5.7.2 of ETSI TS 102 231 [5].

[41] Changes proposed in sections 3.3, 3.4 and 3.5 are proposed as based on suggestions from Stefan Santesson (3xA Security AB) a result of activities within the Swedish single point of contact looking at practical implications of using TSLs.

[42] 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.

Signature algorithm identifier (clause 5.7.3)

This field is REQUIRED and SHALL comply with specifications in clause 5.7.3 of ETSI TS 102 231 [5].

Signature value (clause 5.7.4)

This field is REQUIRED and SHALL comply with specifications in clause 5.7.4 of ETSI TS 102 231 [5]."

3.5 Qualification extension

The section entitled "Qualifications Extension (clause L.3.1)" is replaced by the following:

"**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 that certificates issued by this service are qualified certificates;
- 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."

Annex 1 – Trusted Lists Rationale

Annex 1.1 - On the use of the Trusted List in the context of validating QES or AdES supported by a QC

In practice several difficulties linked to the use of QES and $AdES_{QC,}$ especially in a cross-border use, still persisted and needed to be solved. This includes issues linked to the trust on e-signatures originating from other Member States. Such trust could have been improved by making available information on the supervision or accreditation status of the certification services issuing QC from CSPs established or accredited in Member States. This information is essential to support the validation of QES and AdES supported by QC in a cross-border context. Thus, in order to further support the interoperability and to facilitate the cross-border use of e-signatures, a common template and format for Member States' Supervision / Accreditation Status Lists should be established, hereafter "Trusted List"[43].

In order to validate a received AdES supported by a QC, the receiving party has to check if it is in accordance with the definition and requirements of Directive 1999/93/EC [1], namely that it is:

- an Advanced Electronic Signature (AdES) [44],
- supported by a Qualified Certificate (QC) meeting the requirements of Annex I of Directive 1999/93/EC and provided by a Certification Service Provider (CSP) who fulfils the requirements laid down in Annex II of this Directive,

and in addition, to validate a QES, that it is:

- supported by a Secure Signature Creation Device (SSCD) meeting the requirements of Annex III of Directive 1999/93/EC.

The first piece of trustworthy information to start with for the receiving party validating the e-signature would be the signatory's certificate (chain) supporting it. The data contained in the certificate should allow validating the fact that the certificate is indeed a QC and whether it is supported by a Secure Signature Creation Device (SSCD) in case of a QES. Then as a second source of trust, the Trusted List of the Member State in which the Certification Service Provider (CSP) issuing the signatory's certificate is established or accredited should be used by the receiving party to receive the confirmation of the (supervised/accredited) qualified status of the certificate supporting the received electronic signature.

Unfortunately, at this stage relying on the signatory's certificate (path) may not be enough to get the needed data or it is too complicated (not machine processable, even if manually feasible), due to a number of differences in current requirements and practices linked to the

[43] Throughout the following document 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".

[44] As defined in Art. 2.2 of Directive 1999/93/EC [1].

issuance and use of QC in Member States[45]. Therefore at this stage this information should be available through other means, namely the Trusted List.

Without prejudice to the subsequent simplification of the Trusted List, notably through the use of some common data in the QC[46], the first step to facilitate the validation of QES and $AdES_{QC}$ would be to establish a Trusted List common template and model which would take into account the existing situation and thus contain, in addition to the information on the supervised/accredited certification service status, also information on the QC supporting the signature and whether it is or not created by a Secure Signature Creation Device (SSCD).

Until late 2009, all the existing CSPs issuing QCs, a little more than 100, supervised or accredited in 23 Member States out of the 27 Member States were listed in the national Member States' lists in which they are established or accredited. Nevertheless, there was a wide diversity that can be observed in the information provided in such lists with some lists stating only the registered name of the supervised/accredited CSP issuing QC and other lists containing very detailed information per issuing CA service from supervised/accredited CSPs. Still the majority of those lists did not provide sufficient information to fully support the validation of QES or AdES supported by QC.

By identifying and providing information on the QC (types) issued by supervised/accredited CSPs established in a Member State, a Common Template for Member State's Trusted List would facilitate the validation of an electronic signature by the receiving side by providing information:

- On the fact that the QC supporting the electronic signature is indeed a QC issued by a supervised/accredited CSP issuing QCs,

- On whether the electronic signature is created by an SSCD,

- On the Subject Identification scheme (e.g. Natural vs Legal person, UID scheme), and

- On the supervision/accreditation status of the certification services issuing QC and on the history of this status.

The common Trusted List template would also contain some information on the issuing scheme as well as structured information on the above listed elements.

Annex 1.2 - Information on Supervision / Accreditation schemes

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};

[45] Differences in the actual content of QC issued by CSPs issuing QCs, varying legal requirements for QC profiles, the use of different standards and the wide degree of interpretation of those standards as well as the unawareness of the existence and precedence of some normative technical specifications or standards.

[46] If the information needed for validation could be retrieved in a clear manner from the QC, the trusted list could be simplified and used only to get a confirmation of the qualified status of the issuer's service having issued the certificate supporting the QES or AdES.

- 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 Trusted List with regard to services from CSPs not issuing QCs, the aforementioned sets of information shall be provided at Trusted List level. 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 specific extensions.

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[47]) and that its supervision/accreditation status will be updated accordingly.

Annex 1.3 - Further consideration on the legal importance of the Supervision Model and the provision of information on supervised/accredited CSPs issuing QCs

Directive 1999/93/EC [1] requires Member States to implement *appropriate* supervision systems for CSPs issuing qualified certificates (article 3.3, consideration (13), article 8.1, and 11 of Directive 1999/93/EC), but without specifying how this is to be done. Since Article 5.1 electronic signatures [1], so-called "qualified electronic signatures", (whose reliability by definition relies on qualified certificates (QCs) and thus on the associated supervision) are granted legal equivalence to handwritten signatures without given the relying parties the right to contest this equivalence based on the (in)adequate nature of the supervision scheme, the assumption of legal reliability of supervision schemes is clearly present in the Directive. Challenging this assumption would imply that relying parties would have the right to question the adequacy of supervision systems, and thus of the legal value of qualified signatures. This would run contrary to the letter and spirit of the Directive: it would nullify the cross border value of qualified electronic signatures, as any relying party would always be able to argue that the quality of supervision in another Member State might be inadequate.

This relationship between supervision and the legal value of certificates and signatures also clarifies why a trusted list is needed from a legal perspective. The Directive requires that CSPs issuing QCs are supervised in all Member States. Through this mechanism, supervisory bodies play the role of indirect trust providers.

In the absence of supervisory bodies, any CSP would be able to claim that a certificate would be qualified, without any further prior checks applying and without any possibility of verifying this claim. Since qualified electronic signatures are automatically declared legally equivalent to handwritten signatures, this would create a system based largely on fiction: qualified electronic signatures are considered trustworthy, because they meet a number of requirements including the use of a qualified certificate, which is trustworthy because it is issued by a CSP issuing QCs, who is trustworthy simply because he says so in the

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

certificate. Clearly, this approach of self-declared trustworthiness would not be likely to create a significant degree of trust in foreign CSPs issuing QCs.

This is why Directive 1999/93/EC has adopted a different approach: the practices of CSPs issuing QCs are made subject to an appropriate supervision from a supervisory body, thus ensuring that there is a third party with a governmental mandate which can ensure that the qualified certificate indeed meets the requirements of the Directive. If it were not for the role of this body, no relying party would ever be able to accept foreign signatures (including qualified electronic signatures) without assessing for itself whether the issuing CSP had obeyed all requirements of Directive 1999/93/EC. This would of course not be feasible.

Thus, the Directive creates a clear tiered trust system: qualified certificates inherit trust from the CSP issuing QCs, who inherits trust from the supervision system. This trust system is logical and complete, on one condition: that the relying party can indeed assess whether or not a CSP issuing QC is in fact supervised. If it cannot do so, the trust chain breaks down: the relying party cannot assess whether a certificate is indeed qualified, and is now forced to choose between accepting it anyway without any guarantee whatsoever with regard to its reliability, or rejecting it. In practice, in the absence of a coherent strategy for presenting supervised CSPs issuing QCs at a European level, relying parties who require the use of qualified certificates have no alternative but to reject signatures from unknown CSPs issuing QCs, or encounter a very difficult task in assessing whether a received claimed qualified certificate was issued by a supervised CSP issuing QCs. This is an inevitable result of the insufficient or inconsistent information provided in the previous implementation of the Member State's Trusted List, in the form of the information on the supervision status of CSPs issuing QCs as previously published in the Member States.

This explains why a Trusted List is also necessary from a legal perspective: without a Trusted List, the supervisory bodies lose their function as trust enablers (and can indeed be said to have very little pragmatic use left), and the trust model created by Directive 1999/93/EC no longer functions. Without a Trusted List, relying parties have no reason to trust qualified certificates from CSPs issuing QCs established in other Member States, as there is no guarantee apart from the claim of the CSP that the certificate is indeed qualified.

Directive 1999/93/EC provides the qualified electronic signature with a specific legal value. However, in the absence of a trusted list the relying party cannot know if a signature is really qualified without investing unreasonable auditing resources. Under those circumstances, a relying party could well argue that it would not be required to recognise a qualified electronic signature as such unless there is a way for him to verify its status as a qualified signature; if this possibility does not exist, the Directive logically creates no trust whatsoever. A Trusted List would eliminate this risk: CSPs issuing QCs on the list are by definition supervised, thus their QCs are trustworthy, and thus the legal value of their signatures can no longer be reasonably contested by any relying party. The elimination of this risk is the goal, effect and legal value of the Trust Lists.

Despite the de facto mutual acceptance of Member States' supervision model, the legal obligation on Member States under Directive 1999/93/EC to accept e-signatures cross-borders and the status of qualified electronic signatures (QES) as equal to handwritten signatures, the lack of information about certification service providers issuing QCs (CSP_{QC}) acting in other Member States has led to problems of trusting signatures issued in other Member States. Moreover, different implementations in practice of the existing standards and policies have created further problems for the validation of those signatures.

Annex 2 – Trusted Lists specifications – CD 2009/767/EC as amended by Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States (OJ L 199 of 31.07.2010)

The recitals of CD 2009/767/EC and CD 2010/425/EU are not reproduced here as they can be found in the respective documents and are in essence already provided in the present report Executive Summary. The next sections will provide the Articles of CD 2009/767/EC and its technical annex as modified by CD 2010/425/EU.

[…]

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.

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.

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.

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[48] (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)[49] 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)[50].

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)[51] supported by a Qualified Certificate [52][53].

The proposed Common Template is compatible with an implementation based on the specifications from ETSI TS 102 231[54] that are used to address the establishment, publication, location, access, authentication and trusting of such kinds of lists.

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:

[48] As defined in Art. 2.11 of Directive 1999/93/EC
[49] As defined in Art. 2.10 of Directive 1999/93/EC
[50] As defined in Art. 2.6 of Directive 1999/93/EC
[51] As defined in Art. 2.2 of Directive 1999/93/EC
[52] For an AdES supported by a QC the acronym "$AdES_{QC}$" is used throughout the present document.
[53] 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.
[54] ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

- **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.

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[55].

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

[55] 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.

Expected supervision/accreditation status flow for a single CSP service

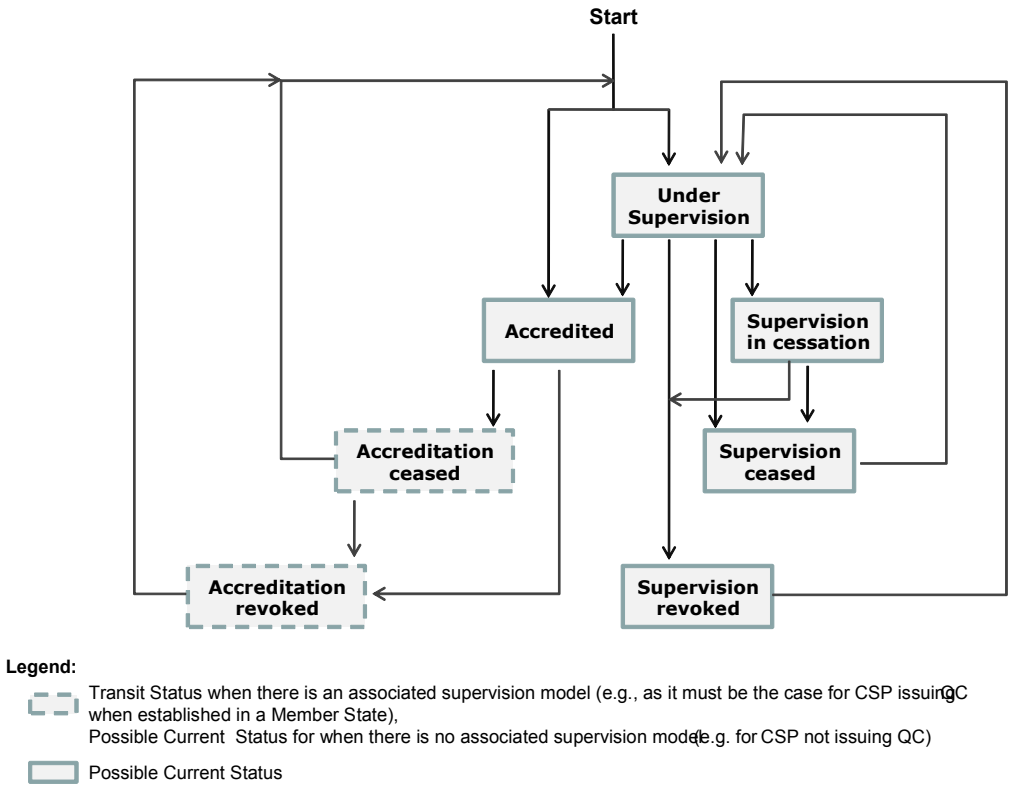


Figure 1

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.

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[56]) 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).

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

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[57] 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[58]. 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")[59] 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).

[57] Refer to ETSI TS 101 862 - Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.
[58] ETSI TS 101 456 - Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
[59] i.e., and as a minimum, an X.509 v3 certificate of the issuing QCA or of an upper CA in the certification path.

Service entry for a listed CSP_{QC}:

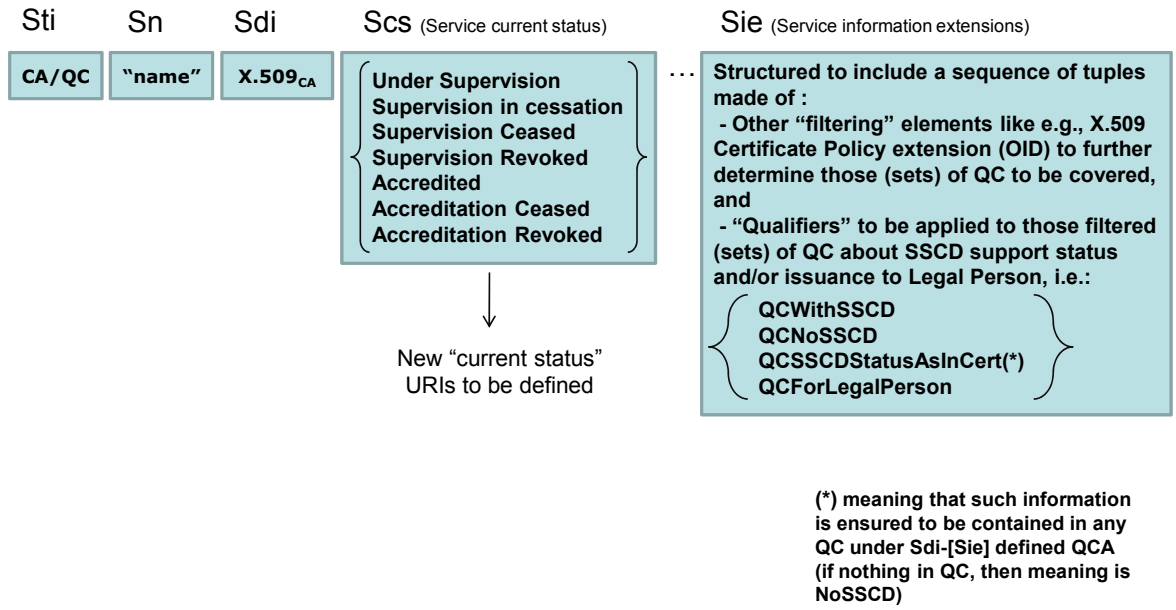


Figure 2: Service entry for a Listed CSP issuing QCs in the TL implemented in TSL format

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).

- 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:

5. 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.

6. 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)

7. 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.

8. 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.

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}.

- **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.

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:

5. Information on the Trusted List and its issuing scheme;
6. 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);
7. 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);
8. 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);
- 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
    iii. 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

iv. 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).

5. 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	Supervision	"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 Accreditation	Accreditation	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 .
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[60].

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.

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.

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)

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.

[60] IETF RFC 2119: "Key words for use in RFCs to indicate Requirements Levels".

TSL type (clause 5.3.3)

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).

Note(1): 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[61] and permitting a parser to determine which form of any following fields[62] 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:

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

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

[61] 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").

[62] 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.

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).

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

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. email 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:

- 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;
  - "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 law.".

- 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:

> 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[63]:
  - 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;

- 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:

[63] 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).

- 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 of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 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.

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.

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 [reference to the present Decision] 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)

  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 [reference to the actual Decision] for further details on the fields, description and meaning for the TSL implementation of the Member States' Trusted Lists.

- 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.

  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 3653 (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.

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[64].

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

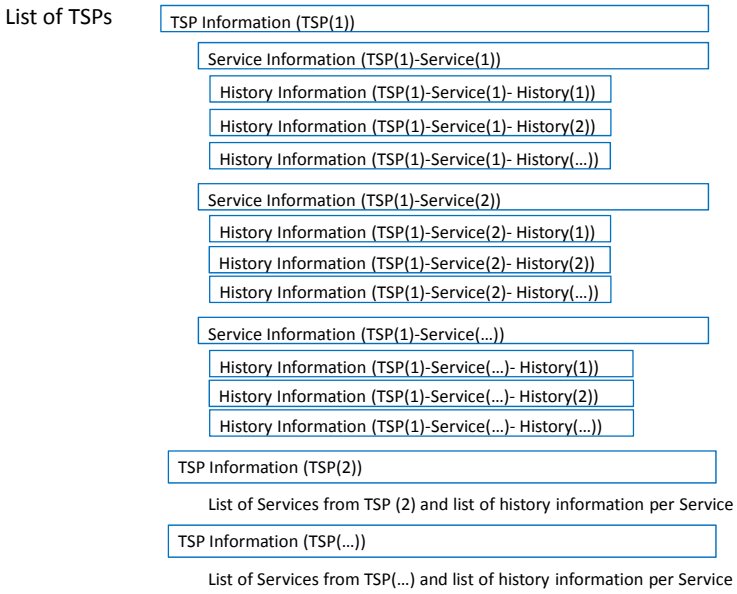
This field is OPTIONAL.

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

[64] IETF RFC 3986: "Uniform Resource Identifiers (URI): Generic syntax".

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).



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. email 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.

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)

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").

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.

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[65]. 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(1): 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

[65] 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.

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

  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[66], 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):

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

[66] 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).

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

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.

- ***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.
- ***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[67] identified in "TSP name" (clause 5.4.1) is found to be in compliance with the provisions laid down in Directive 1999/93/EC.

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

[67] 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).

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:

c) 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);

d) 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[68].

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:

[68] See section 2.2 of the present document.

- (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[69]), 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);

  - **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

[69] 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].

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.

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.

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).

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.

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.

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).

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
...

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[70]. The format of the signature SHOULD be PAdES part 3 (ETSI TS 102 778-3[71]) but MAY be PAdES part 2 (ETSI TS 102 778-2[72]) 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

[70] 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.

[71] 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.

[72] 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.

meet requirements as stated in Annex B of ETSI TS 102 231.[73] Additional general requirements regarding this signature are stated in the following sections.

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.

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.

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.

[73] 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.

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.

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.

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		
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		
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. ”

Chapter III

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:

- 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."

- 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
  - 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.