COMMISSION IMPLEMENTING DECISION

of 14 October 2013

amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States

(notified under document C(2013) 6543)

(Text with EEA relevance)

(2013/662/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

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

Whereas:

(1) 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 [2] obliges Member States to make available information necessary for the validation of advanced electronic signatures supported by a qualified certificate. This information is to be set out uniformly using the so-called 'trusted lists' containing information on certification service providers issuing qualified certificates to the public in accordance with Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [3] and are supervised/accredited by the Member States.

(2) Practical experience with the implementation of Decision 2009/767/EC by Member States has shown that certain improvements are necessary to maximise the benefits of trusted lists. Moreover, the European Telecommunications Standards Institute (ETSI) has published new technical specifications for trusted lists (TS 119 612) that are based on the specifications currently included in the Annex of the Decision, but which, at the same time, make a number of improvements to the existing specifications.

(3) Decision 2009/767/EC should therefore be amended to refer to the ETSI technical specifications 119 612 and to incorporate changes considered necessary to improve and facilitate the implementation and use of trusted lists.

(4) For the purpose of allowing Member States to carry out the required technical changes to their current trusted lists it is appropriate that this Decision should apply as of 1 February 2014.

(5) The measures provided for in this Decision are in accordance with the opinion of the Services Directive Committee,

HAS ADOPTED THIS DECISION:

Article 1

Amendments to Decision 2009/767/EC

Decision 2009/767/EC is amended as follows:

(1) Article 2 is amended as follows:

(a) paragraphs 1, 2 and 2a are replaced by the following:

'1. Each Member State shall establish, maintain and publish, in accordance with the technical specifications set out in the Annex, a "trusted list" containing, as a 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 a machine processable form of the trusted list in accordance with the specifications set out in the Annex. If a Member State chooses to publish a human readable form of its trusted list, that form of the trusted list shall comply with the specifications set out in the Annex.

2a. Member States shall sign electronically the machine processable form of their trusted list in order to ensure its authenticity and integrity. If a Member State publishes a human readable form of the trusted list, it shall ensure that this form of the trusted list contains the same data as the machine processable form and they shall sign it electronically with the same certificate as used for the machine readable form.';

[1] OJ L 376, 27.12.2006, p. 36.
[2] OJ L 274, 20.10.2009, p. 36.
[3] OJ L 13, 19.1.2000, p. 12.

(b) the following paragraph 2b is inserted:

'2b. Member States shall ensure that the machine processable form of their trusted list is accessible at its location of publication at any time, without interruption, except for maintenance purposes.';

(c) paragraph 3 is replaced by the following:

'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 machine processable form of the trusted list;

(b) the location where the machine processable form of the trusted list, is published;

(c) two or more scheme operator public key certificates, with shifted validity periods of at least three months which correspond to the private keys that can be used to sign electronically the machine processable form of the trusted list;

(d) any changes to the information in points (a), (b) and (c).';

(d) the following paragraph 3a is inserted:

'3a. If a Member State publishes a human readable form of the trusted list, information referred to in paragraph 3 shall be notified for the human readable form as well.';

(2) the Annex is replaced by the Annex to this Decision.

Article 2

Application

This Decision shall apply from 1 February 2014.

Article 3

Addressees

This Decision is addressed to the Member States.

Done at Brussels, 14 October 2013.

For the Commission

Michel BARNIER

Member of the Commission

ANNEX

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

GENERAL REQUIREMENTS

1. **Introduction**

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 each Member State provides information about the supervision/accreditation status of the certification services from Certification Service Providers ([1]) (CSPs) who are supervised/accredited by them for compliance with the relevant provisions of Directive 1999/93/EC. This includes the provision of historical information about the supervision/accreditation status of the supervised/accredited certification services.

This information is primarily aimed at supporting the validation of Qualified Electronic Signatures (QES) and Advanced Electronic Signatures (AdES) ([2]) supported by a Qualified Certificate ([3]) ([4]).

The mandatory information in the Trusted List must include, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates (QCs) ([5]) in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3), and Article 7(1)(a)), including, when this is not part of the QCs, information on the QCs supporting an electronic signature and whether or not the signature is created by a Secure Signature Creation Device (SSCD) ([6]).

Additional information on other 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 provided they are either accredited/supervised in a similar way as the CSPs issuing QC or approved under a different national approval scheme. The national approval schemes may in some Member States differ from the supervision or voluntary accreditation schemes applicable for CSPs issuing QCs with regard to applicable requirements and/or the responsible organisation. The terms 'accredited' and/or 'supervised' in the present specifications also cover the national approval schemes but additional information on the nature of any national schemes will be provided by Member States in their Trusted List, including clarification on the possible differences with the accreditation/supervision schemes applied to CSPs issuing QCs.

The Common Template relies on ETSI TS 119 612 v1.1.1 ([7]) (hereafter referred to as ETSI TS 119 612) that addresses the establishment, publication, location, access, authentication and integrity of such lists.

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

The Common Template for a Member State Trusted List is structured according to ETSI TS 119 612 into the following categories of information:

1. A trusted list tag facilitating the identification of the Trusted List during electronic searches;

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

3. A sequence of fields containing 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 have no content thereby denoting the absence of any supervised or accredited CSP in the associated Member State for the purposes of the Trusted List);

4. For each listed CSP, the details of its specific trust services, the current status of which are recorded within the Trusted List, are provided as a sequence of fields unambiguously identifying supervised/accredited certification services provided by the CSP and their current status (this sequence must have a minimum of one entry);

([1]) As defined in Article 2(11) of Directive 1999/93/EC.
([2]) As defined in Article 2(2) of Directive 1999/93/EC.
([3]) For an AdES supported by a QC the acronym '$AdES_{QC}$' is used throughout the present document.
([4]) 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.
([5]) As defined in Article 2(10) of Directive 1999/93/EC.
([6]) As defined in Article 2(6) of Directive 1999/93/EC.
([7]) ETSI TS 119 612 v1.1.1 (2013-06) – Electronic Signatures and Infrastructures (ESI); Trusted Lists.

5. For each listed supervised/accredited certification service, the information on the history of this status, when applicable;

6. The signature applied on the Trusted List.

In the context of a CSP issuing QCs, the structure of the Trusted List and in particular the service information component (as per point 4 above) allows for complementary information in service information extensions to compensate for those situations where insufficient (machine processable) information is available within 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 Certification Authority (CA) to issue several types of end-entity certificates, both qualified and non-qualified.

In the context of certificate generation (CA) services, the number of service entries in the list for a CSP may be reduced where one or several upper CA services exist within the CSP's PKI (e.g. in the context of a hierarchy of CAs from a Root CA down to several issuing CAs) by listing such upper CA services and not the CA services issuing end-entity certificates (e.g. listing the CSP Root CA only). However in those cases, the status information applies to the whole hierarchy of CA services below the listed service and the principle of ensuring the unambiguous link between a CSP_{QC} certification service and the set of certificates intended to be identified as QCs has to be maintained and ensured.

2.1. *Description of information in each category*

1. Trusted List Tag

2. Information on the Trusted List and its issuing scheme

The following information is part of this category:

— A Trusted List **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 **scheme operator (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**,

— Trusted List **next planned update.**

3. Unambiguous identification information about every CSP supervised/accredited under the scheme

This set of information includes at least the following:

— The CSP organisation name as used in formal legal registrations (including 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 additional information can be downloaded.

4. 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 includes at least the following for each certification service from a listed CSP:

— Service type identifier: 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),

— Service (trade) name: (trade) name of this certification service,

— Service digital identity: An unambiguous unique identifier of the certification service,

— Service current status: An identifier of the current status of the service,

— The current status starting date and time,

— Service information extension, when applicable: Additional information on the service (e.g. directly included or included by reference to a location from which information can be downloaded): service definition information provided by the scheme operator, access information with regards to the service, service definition information provided by the CSP and service information extensions. E.g. for CA/QC services, an optional sequence of tuples of information, each tuple providing,

  — Criteria to be used to further identify (filter) within the identified trust service that precise set of service outputs (e.g. set of (qualified) certificates) for which additional information is required/provided with regards to its status, the indication of the SSCD support and/or issuance to a legal person, and

  — The associated 'qualifiers' providing information on whether the set of service outputs identifies certificates to be considered as qualified and/or whether the identified qualified certificates from this service are 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 historical information about his status

6. A signature computed for authentication purposes over all fields of the TL except the signature value itself

3. **Guidelines for editing entries in the Trusted List**

3.1. *Status information on supervised/accredited certification services and their providers in a single list*

The Trusted List of a Member State means 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 is the single instrument to be used by the relevant Member State to provide information on the supervision/accreditation status of certification services and their providers:

— **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 Article 3(3), Article 8(1), Article 11, recital 13 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11, recitals 4, 11, 12 and 13).

— **CSPs not issuing QCs**:

— They may fall under a 'voluntary accreditation' system (as defined in and in accordance 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 that Directive and possibly with national provisions with regard to the provision of certification services (in the sense of Article 2(11) of Directive 1999/93/EC).

— 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.

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 that are supervised/accredited by the Member State. The Trusted List shall include at least those CSPs issuing QCs. The Trusted List may also indicate the status of other certification services supervised or accredited under a nationally defined approval scheme.

3.2. *A single set of Supervision/Accreditation status values*

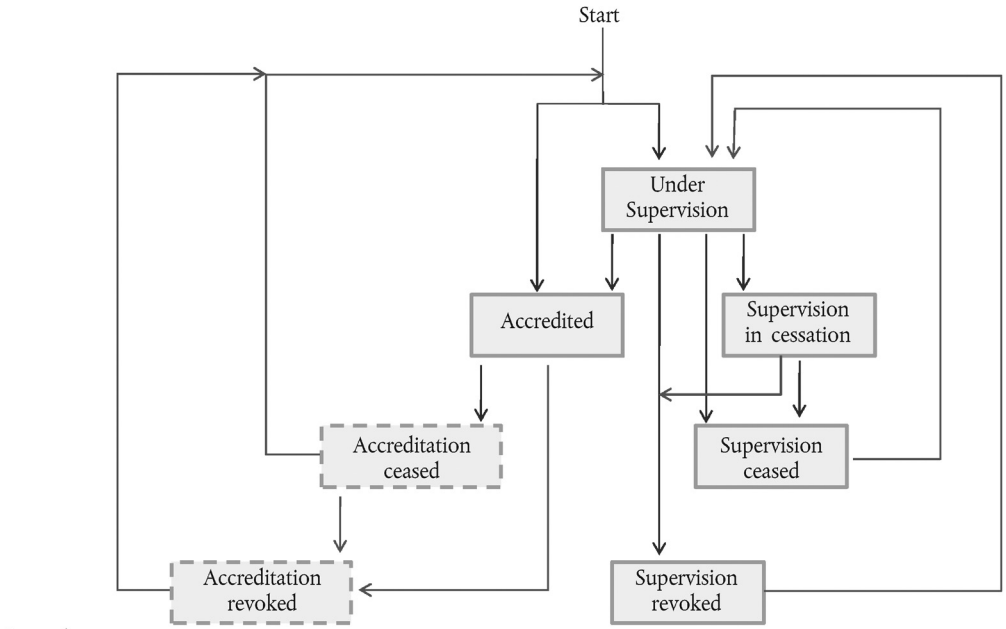
In the Trusted List, the fact that a service is currently either 'supervised' or 'accredited' is given by the value of its current status. In addition to that, a supervision or accreditation status can be positive ('under supervision', 'accredited', 'supervision in cessation'), ceased ('supervision ceased', 'accreditation ceased'), or even revoked ('supervision revoked', 'accreditation revoked') and be set to the corresponding value. Throughout its lifetime, the same certification service may move from a supervision status to an accreditation status and vice versa [1].

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

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

Figure 1

Expected supervision/accreditation status flow for a single CSP service



Legend:

Transit Status when there is an associated supervision model (e.g. for a CSP issuing QC accredited and supervised in the Member State in which it is established),
Possible Current Status when there is no associated supervision model (e.g. for a CSP accredited in a Member State in which it is not established)

Possible Current Status

When established in a Member State, a certification service issuing QCs must be supervised (by the Member State in which it is established) and may be voluntarily accredited. The status value of such a service when listed in a Trusted List must have one of the above depicted status values as 'current status value' in accordance with its actual status and must change, when applicable, according to the status flow depicted above. However, 'Accreditation ceased' and 'Accreditation revoked' must both be 'transit status' values when the corresponding CSP_{QC} service is listed in the Trusted List of the Member State in which it is established, as such a service must be supervised by default (even when not or no longer accredited); when the corresponding service is listed (accredited) in another Member State than the one it is established in, these values may be final values.

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 Article 2(11) of Directive 1999/93/EC) must categorise such approval scheme(s) under the following two categories:

— 'voluntary accreditation' as defined and regulated in Directive 1999/93/EC (Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11, recitals 4, 11, 12 and 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 must have one of the above depicted status values as its 'current status value' (see Figure 1) in accordance with its actual status and must evolve, when applicable, according to the status flow depicted above.

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 Trusted List with regard to services from CSPs not issuing QCs, the aforementioned sets of information shall be provided at Trusted List 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 5.5.9.4) as part of 'Service information extensions' (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 must be used for one single certification service and that its supervision/accreditation status must be updated accordingly.

3.3. *Trusted List entries aiming at facilitating the validation of QES and $AdES_{QC}$*

The most critical part of the creation of the Trusted List is the establishment of the mandatory part of the Trusted List, namely the 'List of services' per CSP issuing QCs, in order to reflect correctly the exact situation of each 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).

The required information might include information other than the 'Service digital identity' of a single (Root) CA, in particular information identifying the QC status of certificates issued by such a CA service, 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 Trusted List must therefore take into account the current profile and certificate content in each issued QC, per CSP_{QC} service covered by the Trusted List.

Ideally each issued QC should include the ETSI defined QcCompliance [1] statement when it is claimed that it is a QC and should include the ETSI defined QcSSCD statement when it is claimed that it is supported by an SSCD to generate eSignatures, and/or that each issued QC includes one of the QCP/QCP+ certificate policy Object Identifiers (OIDs) defined in ETSI EN 319 411-2 [2]. The use by CSPs issuing QCs of different standards as references, the wide degree of inter-pretation 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.

[1] Refer to ETSI EN 319 412-5 (Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile) for the definition of such a statement.

[2] ETSI EN 319 411-2 — Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

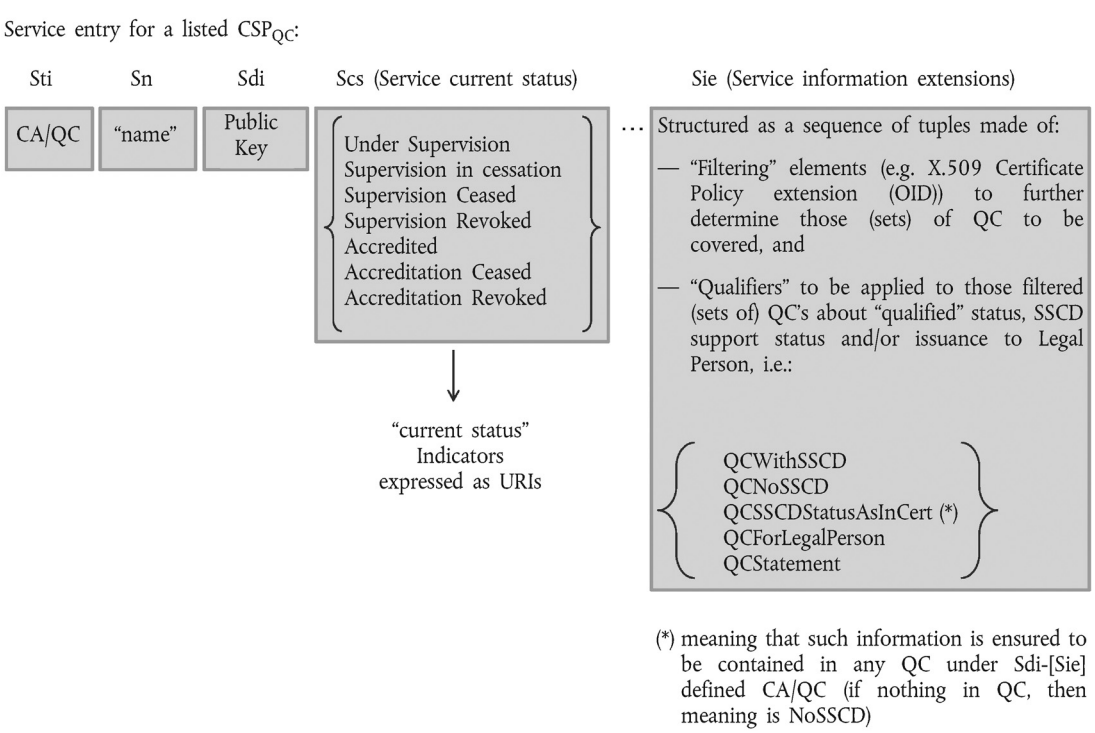
Completing the 'Service type identifier' ('Sti'), 'Service name' ('Sn'), and 'Service digital identity' ('Sdi') fields of the service entry in the Trusted List with information provided in the 'Service information extensions' ('Sie') field allows for the full determination of a specific type of qualified certificate issued by a listed CSP certification service issuing QCs and provides information about whether or not it is supported by an SSCD (when such information is missing in the issued QC). A specific 'Service current status' ('Scs') information is associated with 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 or not 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 indicate that those QCs must be considered as supported by an SSCD, the 'Sie' field should be used (this also indicates that this information is guaranteed by the CSP issuing QCs and supervised/accredited by the Supervisory or Accreditation Body respectively).

Figure 2

Service entry for a listed CSP service issuing QCs in the Trusted List

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



The present Trusted List common template technical specifications allow for the use of 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 public key (as a minimum) of a CA issuing QCs,

— For CA/QC services, optional 'Service information extension' ('Sie') information that allows for the inclusion of a number of specific service-related items of information relating to revocation status of expired certificates, additional characteristics of QCs, takeover of CSP by another CSP and other additional service information. For example, the additional characteristics of QCs are represented by 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 set of qualified certificates for which additional information is required/provided with regard to the indication of the 'qualified' status, the SSCD support and/or issuance to a Legal Person, and

  — The associated information ('qualifiers') on whether this set of qualified certificates is to be considered as 'qualified', 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.

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

The **general editing guidelines** are:

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

2. If it is ensured (guarantee provided by CSP_{QC} and supervised/accredited by SB/AB) that, for a listed service identified by a 'Sdi', any QC not supported by an SSCD does contain the QcCompliance statement and/or the QCP OID, and does 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 does not have 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 a certificate that is supported by an SSCD 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 qualification 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 public key for a CA/QC type certification service, i.e. per Certification Authority (directly) issuing QCs. In some exceptional circumstances and carefully managed conditions, the Member State's Supervisory Body/Accreditation Body may decide to

use, as the 'Sdi' of a single entry in the list of services from this listed CSP, the public key of a Root or Upper level CA within the CSP's PKI (e.g. in the context of a CSP's hierarchy of CAs from a Root CA down to several issuing CAs) instead of listing all sub-ordinate issuing CA services (i.e. listing a Certification Authority not directly issuing end-entity QCs but certifying a hierarchy of CAs down to CAs issuing QCs to end-entities). The consequences (advantages and disadvantages) of using such Root CA or Upper CA public key as 'Sdi' value in a Trusted List service entry must be carefully considered when implemented by Member States. Moreover, when using this authorised exception to the default principle, the Member State must provide the necessary documentation to facilitate certification path building and verification. As an example, 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 none of the QC issued under this Root CA is supported by an SSCD. If there are QCs that are actually supported by an SSCD but with no machine processable statement indicating such support included in the certificates, 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 Trusted List should make use of the 'Sie' field and associated 'Qualifications Extension', e.g. providing filtering information to identify set(s) of certificates through use of 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 associating explicit 'SSCD support information' to those identified (filtered) set(s) of certificates through the use of 'Qualifiers'.

The **general usage guidelines** for electronic signature applications, services or products relying on a Trusted List compliant with 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 machine processable QcStatement (i.e. QcCompliance) and/or ETSI defined QCP(+) OIDs (and this is ensured by Supervisory/Accreditation Body, see above 'general editing guidelines')

Note: if no 'Sie' 'Qualifications Extension' information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related 'Sie' 'Qualifications Extension', 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. QcCompliance, 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' 'Qualifications Extension' information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this 'Sie' 'Qualifications Extension' information, 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 the qualified status, the '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 qualified status: 'QCStatement' meaning the identified certificate(s) is(are) qualified,

    AND/OR

  — 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'

3.5. *Services supporting 'CA/QC' services but not part of the 'CA/QC' 'Sdi'*

Certificate validity status services related to QCs and for which the certificate validity status information (e.g. CRLs and OCSP responses) is signed by an entity whose private key is not certified under a certification path leading to a listed CA issuing QCs ('CA/QC') shall be included in Trusted List by listing those certificate validity status services as such in the TL (i.e. with a service type '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).

The Trusted List shall include certificate validity status services when related location information for such services is not present in the end-entity certificates to which the certificate validity status services apply.

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	(1) a certification service provider that creates and assigns public key certificates; or (2) a technical certificate generation service that is used by a certification service provider that creates and assign public key certificates. *NOTE*: See clause 4 of EN 319 411-2 [1] for further explanation of the concept of certification authority.
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	Refers to supervision provided for in Article 3(3) of Directive 1999/93/EC. Directive 1999/93/EC 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 that 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.

Term	Acronym	Definition
Trust-service Status List	TSL	Form of a signed list used as the basis for presentation of trust service status information according to the specifications laid down in the ETSI TS 119 612.
Trust Service		Service which enhances trust and confidence in electronic transactions (typically, but not necessarily, using cryptographic techniques or involving confidential material) (ETSI TS 119 612). *NOTE*: This term is used with a broader application than certification service issuing certificates or providing other services related to electronic signatures.
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, Certificate Revocation Lists (CRLs), Time Stamp Tokens (TSTs) and Online Certificate Status Protocol (OCSP) responses.
Qualified Electronic Signature	QES	An AdES supported by a QC and which is created by a secure signature creation device 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.

([1]) EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

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

CHAPTER I

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

The present specifications are relying on the specifications and requirements stated in ETSI TS 119 612 v1.1.1 (here after referred to as ETSI TS 119 612).

When no specific requirement is stated in the present specifications, requirements from ETSI TS 119 612 clauses 5 and 6 SHALL apply entirely. When specific requirements are stated in the present specifications, they SHALL prevail over the corresponding requirements from ETSI TS 119 612. In case of discrepancies between the present specifications and specifications from ETSI TS 119 612, the present specifications SHALL be the normative ones.

Scheme operator name (clause 5.3.4)

This field SHALL be present and SHALL comply with the specifications from TS 119 612 clause 5.3.4.

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

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 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 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 Trusted List, including in the scheme-specific information indicated by the 'Scheme information URI' (clause 5.3.7).

Scheme name (clause 5.3.6)

This field SHALL be present and SHALL comply with the specifications from TS 119 612 clause 5.3.6 where the following name SHALL be used for the scheme:

'EN_name_value' = 'Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Scheme Operator's Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.'

Scheme information URI (clause 5.3.7)

This field SHALL be present and SHALL comply with the specifications from TS 119 612 clause 5.3.7 where the 'appropriate information about the scheme' SHALL include as a minimum:

— Introductory information 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 the text below, in which the character string '[*name of the relevant Member State*]' SHALL be replaced by the name of the relevant Member State:

'The present list is the '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,

— allowing for a trusted validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including, when this is not part of the QCs, 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 compliance 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 Article 3(3), Article 8(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 at a national level on a voluntary basis.'

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

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

  — 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 be provided on a voluntary basis such as:

— 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.

Scheme type/community/rules (clause 5.3.9)

This field SHALL be present and SHALL comply with the specifications from TS 119 612 clause 5.3.9 and SHALL include at least two URIs:

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

  URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

  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 implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's 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, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 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.

[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 applicable to CSPs not issuing QCs. Those sets of information shall be provided at Trusted List 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).

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 compliance 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 Article 3(3), Article 8)(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 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 Article 2(11) of Directive 1999/93/EC). 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 Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on 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 EN 319 412-5 defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or EN 319 411-2 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

Note: if no 'Sie' 'Qualifications Extension' information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related 'Sie' 'Qualifications Extension' information, 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. QcCompliance, QcSSCD, etc.) 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' 'Qualifications Extension' information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this 'Sie' 'Qualifications Extension' information, 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 the qualified status, the '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 qualified status: 'QCStatement' meaning the identified certificate(s) is(are) qualified,

AND/OR

— to indicate the nature of the SSCD support:

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

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

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

AND/OR

— to indicate issuance to Legal Person:

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

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

Please refer to the Technical specifications for a Common Template for the 'Trusted List of supervised/accredited Certification Service Providers' in the Annex of Commission Decision 2009/767/EC for further details on the fields, description and meaning for the 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/TrustedList/schemerules/CC where CC = the ISO 3166-1 ([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 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 (clause 5.5.9) are used for this purpose.

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

TSL policy/legal notice (clause 5.3.11)

This field SHALL be present and SHALL comply with the specifications from TS 119 612 clause 5.3.11 where the policy/legal notice concerning the legal status of the scheme or legal requirements met by the scheme under the jurisdiction in which it is established and/or any constraints and conditions under which the trusted list is maintained and published SHALL be a multilingual character string (plain text) made of two parts:

1. A first mandatory part, common to all Member States' Trusted Lists (with UK English 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 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.

([1]) ISO 3166-1:2006: 'Codes for the representation of names of countries and their subdivisions Part 1: Country codes'.

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

2. A second, optional, part, specific to each Trusted List (with UK English 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).

CHAPTER II

CONTINUITY OF TRUSTED LISTS

Certificates to be notified to the Commission under Article 3(c) of the present Decision SHALL be issued in such a way that they:

— have as a minimum three months between their validity dates,

— are created on new key pairs as no previously used key pair are to be re-certified.

In case of a compromise or decommissioning of ONE of the private keys corresponding to the public key that could be used to validate the trusted list's signature and that has been notified to the Commission and is published in the Commission's central lists of pointers, Member States SHALL:

— re-issue, without any delay, a new trusted list signed with a non-compromised private key in case the published trusted list was signed with a compromised or decommissioned private key,

— promptly notify to the Commission the new list of public key certificates corresponding to the private keys that could be used to sign the trusted list.

In case of compromise or decommissioning of ALL the private keys corresponding to the public keys that could be used to validate the trusted list's signature and that have been notified to the Commission and are published in the Commission's central lists of pointers, Member States SHALL:

— generate new key pairs that could be used to sign the trusted list and their corresponding public key certificates,

— re-issue, without any delay, a new trusted list signed with one of those new private keys and whose corresponding public key certificate is to be notified,

— promptly notify to the Commission the new list of public key certificates corresponding to the private keys that could be used to sign the trusted list.

CHAPTER III

SPECIFICATIONS FOR THE HUMAN READABLE FORM OF THE TRUSTED LIST

If a human readable form of the trusted list is established and published, it SHOULD be provided in the form of a Portable Document Format (PDF) document according to ISO 32000 ([1]) that MUST be formatted according to the profile PDF/A (ISO 19005 ([2])).

The content of the PDF/A based human readable form of the trusted list SHOULD comply with the following requirements:

— The structure of the HR form SHOULD reflect the logical model described in TS 119 612,

— 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 (e.g. 'A Certification authority issuing public key certificates.'),

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

([1]) ISO 32000-1:2008: Document management – Portable document format – Part 1: PDF 1.7
([2]) ISO 19005-2:2011: Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2)

— The following fields and corresponding values of the digital certificates present in the 'Service digital identity' field SHOULD, as a minimum, be 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 MUST be signed by the Scheme Operator according to PAdES Signatures baseline profile [1].

[1] ETSI TS 103 172 (March 2012) - Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile