Study on Cross-Border Interoperability of eSignatures

(CROBIES)

"Trusted Lists"

User'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 2-2 **Trusted Lists – User's Guide**
Project reference:	CROBIES
Document archival code:	INFSO-CROBIES-FINALREPORT-WP2-2-SEALED-31072010_v1

Version control

Version	Date	Description / Status	Responsible
V1	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

1 INTRODUCTION 4

1.1 CROBIES 4
1.2 Target Audience 4
1.3 Executive Summary 5

2 TRUSTED LISTS 7

2.1 Scope of the Trusted Lists 7
2.2 Trusting Trusted Lists – The trust model 11
2.3 Structure of the common template for the Trusted Lists 13
2.4 Listed TSP Services 15
2.4.1 Overview 15
2.4.2 Editing guidelines for CSP services entries 19
2.4.3 General usage guidelines 21
2.5 Trusted Lists versus Certificate Trust Stores 24

3 USING TRUSTED LISTS TO VALIDATE ADES$_{QC}$ AND QES 25

3.1 Reference Verification Process of a Certificate against a Trusted List 25
3.2 Existing tools 29

4 CONCLUSIONS AND RECOMMENDATIONS 30

ANNEX 1 – TRUSTED LISTS RATIONALE 31

Trusted Lists

User'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 any interested electronic signature stakeholder or third party willing to better understand the usage of "Trusted Lists of supervised/accredited Certification Service Providers" (in particular issuing QCs) as specified by CD 2009/767/EC [6] as amended by Decision 2010/425/EU [7] amending CD 2009/767/EC. In particular it addresses any party that has to implement QES or $AdES_{QC}$ validation, whether when providing validation tools or services, or when acting as a relying party wishing to parameter its electronic signature application.

[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].

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 support the publication of this information, enhancing the interoperability and facilitating the cross-border use of e-signatures, through a common template and format of Trusted Lists.

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 on the one hand 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 other hand,** on the fact that it is indeed a QC and whether or not it supported by an SSCD (whether those CSP statements are part of the certificate or the information is provided in the Trusted List itself).

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].

[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.

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

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 [6] and [7] 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 is 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 as Decision 2010/425/EU [7] 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.

The compiled provisions and technical requirements from CD 2009/767/EC as amended by Decision 2010/425/EU are provided as an unabridged version for information purposes in Annex 2 of the CROBIES WP2-1 report titled "Trusted List – Implementer's Guide".

[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 aim of the present report “Trusted Lists – User’s Guide” is to provide a general guidance on how Trusted Lists should be used by relying parties when validating $AdES_{QC}$ or QES, or more generally when validating QC’s.

Section 2 provides important background information the reader should read to understand the way Trusted Lists can and should be used to further facilitate the verification of electronic signatures and in particular QES or $AdES_{QC}$. Trusted Lists are significantly different from CA Certificate Trust Stores in terms of nature but also in terms of usage. This section aims to highlight these differences.

Finally Section 3 provides a high level reference verification process of a certificate against a Trusted List and discusses one of the latest, visible and interesting applications developed so far to validate electronic signatures and supporting certificates against such Trusted Lists.

Section 4 provides some conclusions and recommendations.

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 [6] [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 per Member State must be established, published and maintained 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 [1].

Trusted List of supervised/accredited CSPs

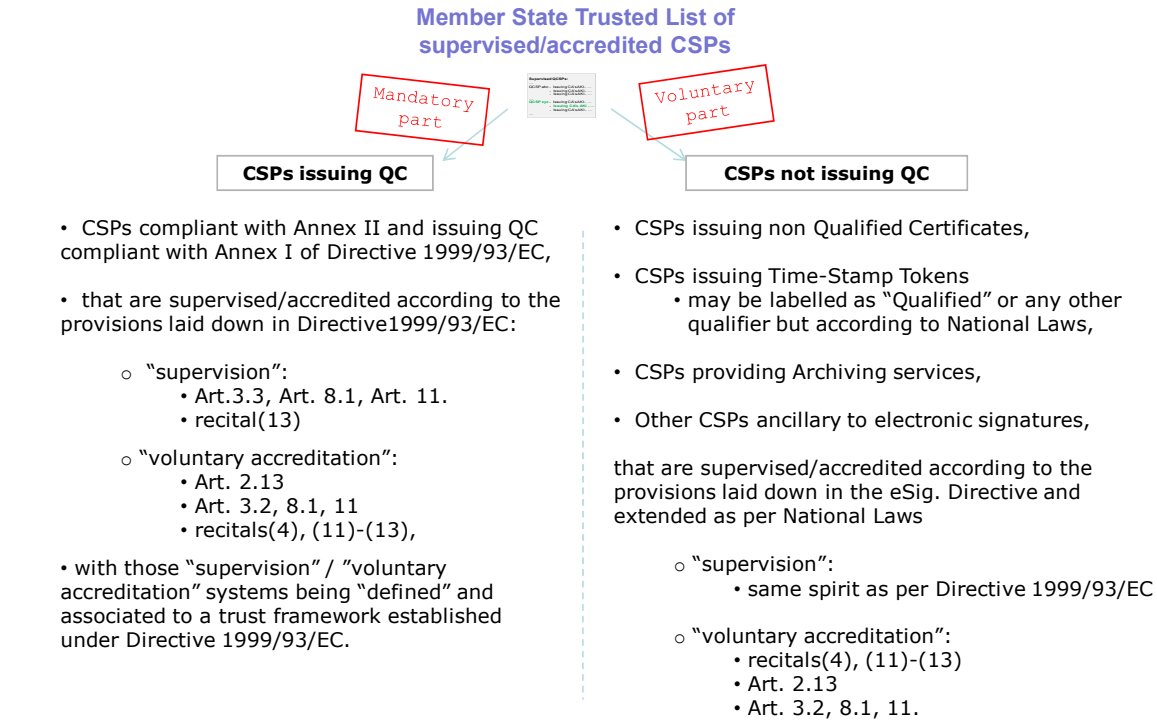


Figure 1

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 [1], 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. 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.

[8] As defined in Art. 2.10 of Directive 1999/93/EC [1].
[9] As defined in Art. 2.6 of Directive 1999/93/EC [1].

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 in [6] as amended by [7].

Expected supervision/accreditation status flow for a single CSP service

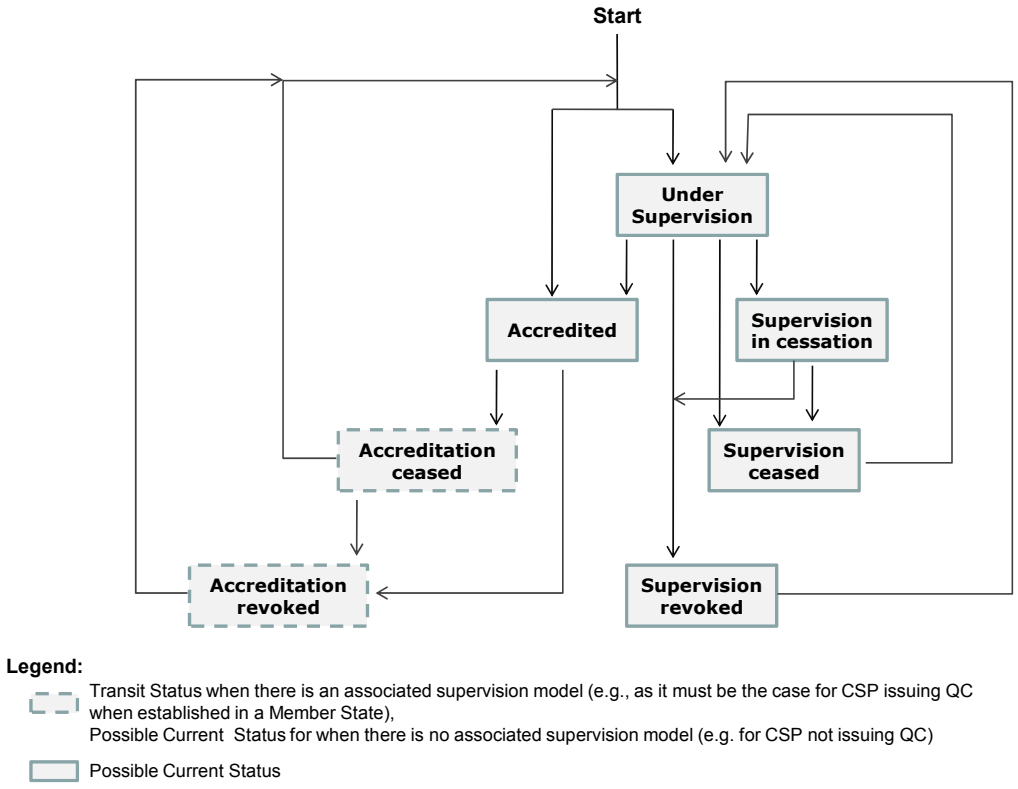


Figure 2

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.

The meaning of the “Service current status” values defined in [6] [7] is 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.

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 amended by Decision 2010/425/EU, 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 Trusting Trusted Lists – The trust model

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

- 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 (e.g. TLS, SSL) in order to ensure its authenticity and integrity.

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).

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

[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.

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;

  (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)[14] and in a signed machine processable format[15].

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[16], 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 information contained in each national list.

The certificates used by the European Commission Scheme Operator when respectively signing the machine-processable version and securing the human readable version of the

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

Compiled List are published in the Official Journal of the European Commission[17] to ensure a trustworthy verification of the integrity and authenticity of the Member States Trusted List location and associated public key certificates to be used to authenticate the national Trusted Lists.

With regards to the type of public key certificates associated to the Trusted List signing private keys, 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.

2.3 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.

---

[17] The authenticity and integrity of the machine processable version of the compiled list is ensured through an electronic signature supported by a digital certificate. The certificate was published **on page 16 of the Official Journal of the European Union C 45 of 23.02.2010.**

The authenticity and integrity of the human readable version of the compiled list is ensured through an TLS/SSL secured connection supported by a digital certificate. The certificate was published **on page 15 of the Official Journal of the European Union C 57 of 09.03.2010.**

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, notably 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:

- The “Service type identifier” (“**Sti**”), 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);
- This “Sti” can be further completed by an extension (“Service information extension:additionalServiceInformation” – “**Sie:aSI**”) that may be used to further

precise the type of service (e.g. “CA/QC:RootCA-QC” indicates that the listed service is a RootCA rootsigning CAs issuing QCs)
- The “Service name” (“**Sn**”), i.e. the (trade) name of this certification service;
- The “Service digital identity” (“**Sdi**”), an unambiguous unique identifier of the certification service being as a minimum the X.509v3 certificate of this certification service (e.g. for CA, Root-CA, TSA, OCSP and CRL issuing services);
- 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 (“Service information extension:Qualifications” – “**Sie:Q**”) of tuples of information used to identify (through specific “criteria”) those certificates issued by the listed certification service that need further clarification with regards to their qualified status and SSCD support (through pre-defined “qualifiers”), 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.

2.4 Listed TSP Services

2.4.1 **Overview**

In order to better understand how to use Trusted Lists when validating $AdES_{QC}$ and QES, it is worth better understanding how the relevant information is organized in the Trusted List with regards to the listed certification services, in particular those issuing QCs, and how this information can be used to further enhance confidence in the fact that a claimed QC is indeed a QC issued by a supervised or accredited CSP certification service, and in the fact that whether or not the private key associated to the QC certified public key resides in a SSCD.

Per listed CSP in the Trusted List, a list of services is provided as 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.

As the retention of historical information about listed services is required under CD 2009/767/EC specifications to be equal or greater than 10 years, 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 specified in the "Historical information period" field.

The certification service entries listed in a Trusted List conform to Trusted Lists specifications [6] [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.

This "List of services" (e.g. issuing QCs as a minimum) provided per CSP, is meant to correctly reflect the exact issuing situation of each supervised/accredited QC-issuing certification service and to provide sufficient information 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" (i.e. the X.509v3 certificate) 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 in the European Union 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 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.

[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.

When there is an identified lack of machine processable information with regards to the QC statement and the SSCD support statement in the content of QC issued by a specific supervised or accredited service, the Trusted List corresponding service entry basic information (namely the “Service type identifier” (“Sti”), “Service name” (“Sn”), and "Service digital identity" ("Sdi")[20] fields) is completed with information provided in the "Service information extensions" ("Sie") field. This additional information allows 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 “Service current status” (“Scs”) information is of course associated to this entry. This is depicted in Figure 3 below.

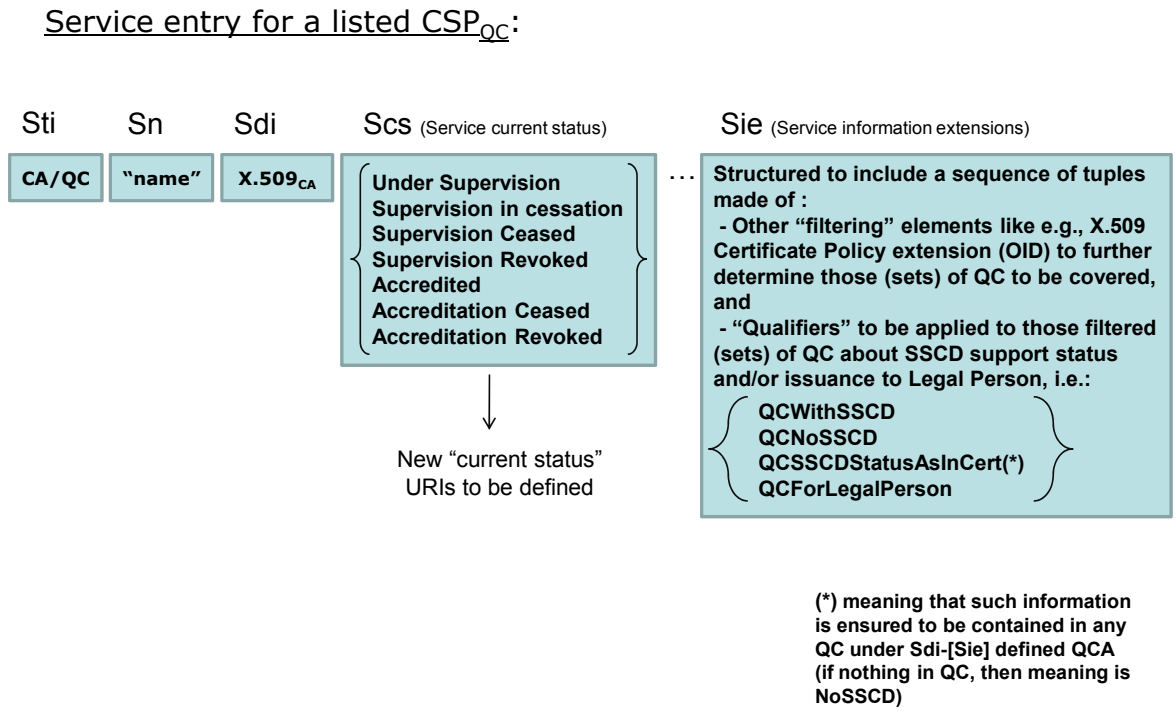


Figure 3: Service entry for a Listed CSP issuing QCs in a Member State Trusted List

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.

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 must 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).

[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.

2.4.2 **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). Trusted Lists specifications [6][7] 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 [6][7]) are:
>
> - For what is predefined in [6][7]
>   - 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.

In particular 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.

2.4.2.1 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”.

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

Provisions stated in Section 2.4 of Annex from Trusted Lists specifications [6][7] 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.*
>
> *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.*

2.4.3 General usage guidelines

The **general usage guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List established according to the CD 2009/767/EC 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)

[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.

- 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”

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 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 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.

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[22] 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 with regards to the that the private key associated with the public key in the certificate resides within a Secure Signature Creation Device, 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

[22] For further details on encoding specifications and in particular on the way to express Criteria and on pre-defined qualifiers, please refer to CD 2009/767/EC.

a lack of information with regards to the SSCD support claim. This lack of information is compensated by the "**QCSSCDStatusAsInCert**" meaning that for those end-entity 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 (compensated) as the private key associated with the public key in those certificates **does not** reside within a Secure Signature Creation Device.[23]

2.5 Trusted Lists versus Certificate Trust Stores

Trusted Lists are not CA certificate trust stores. The scope, purpose and philosophy of use is quite different.

CA Certificate Trust Stores are containers or directories in which CA certificates are stored that are trusted according to a determined policy. It can be (Root) CA certificates that are trusted and distributed within specific Web Browser software's, CA certificates that are trusted in the context of an Enterprise application domain, or Trusted Publishers CA certificates that are trusted by Software Restriction policies or even a set of certificates from end-entities that are trusted by a relying party. Those CA certificate Trust Stores are usually meant to be used jointly with the certification path validation process that aims to identify a valid path from the end-entity certificate (e.g. a signature verification certificate in the context of electronic signatures) up to a Trusted Root CA (or Trust Anchor)[24], potentially through one or more intermediate CAs. However the trust level or granularity that can be associated to such CA Trust Stores are limited to the level of the CA certificate that is so trusted, meaning that whatever type of certificate issued by or "below" such a Trusted Anchor is out of scope as the main objective of such Trust Store is to determine whether or not the stored CA certificate is trustworthy or not, not to determine whether the issued end-entity certificate is trustworthy or not.

The scope of Trusted Lists is quite different. It is not aimed to support the building or validation of a determined certification path from an end-entity certificate up to a Trust Anchor but to facilitate determining whether or not an end-entity certificate is a QC, and whether or not the associated private key resides in an SSCD.

Trusted Lists are not national store of "Trusted Root CAs" or "Trust Anchors" as it is understood when validating certificates or building a certification path. Trusted Lists are not meant to compensate the lack of information with regards to, or to assist in, building a certificate path/chain up to whatever "Trust Root" or "Trust Anchor" that may be considered as relevant for a signer or a signature verifier according to whatever signature validation policy they may rely on.

Trusted Lists are to be used to facilitate the validation of QES and $AdES_{QC}$ in the sense that they allow verifying the fact that the claimed QC supporting the QES or AdESQC to be verified is indeed a QC issued by a CA/QC service from a CSP that is supervised or accredited by a Member State[25].

The use of Trusted Lists, with regards to QC, should be considered independently and in

[23] Certificates issued under the listed CA/QC::RootCA-QC certification service that do not contain at least one of the listed OID will be considered as QC or as public key certificates for which the private key resides in an SSCD when they do contain the appropriate ETSI defined machine-processable information (i.e. QCP certificate policy OID, QcCompliance statement, QCP+ certificate policy OID and/or QcSSCD statement).

[24] Usually expected to be found in a Certificate Trust Store.

[25] Note that the same principle applies similarly for listed services other than CA/QC but in the context of the present section one will focus on CA/QC type of certification services.

addition to the requirements a verifier may have with regards to the certification path or the trust anchor when verifying a QES or $AdES_{QC}$. Such certification path requirements may come (e.g. as from a signature validation policy) in addition to the fact that he must verify that indeed the signer's certificate is a QC and whether or not it is supported by an SSCD.

In order to validate that a received electronic signature is a QES or an $AdES_{QC}$, there is strictly speaking no need to care about certification path building or validation up to a Trust Anchor (while this might be required by the relying party signature validation policy) nor to rely or build a Certificate Trust Store . From the content of claimed QC supporting the received QES or $AdES_{QC}$, and the applicable Trusted List, relying parties do have enough information to assess whether or not the received electronic signature is a QES or an $AdES_{QC}$ or none of both. In addition to this check, it may be still necessary for the relying party to further build and validate a certification path to comply with some additional specific and related signature validation policies.

The basic process for using TL as a facilitation tool to validate whether or not an electronic signature is a QES or $AdES_{QC}$ is the following:

- Once the cryptographic basic verification of the signature is done,
- Once a (trusted) time reference is found by the relying party,
- Once a sufficient period of time elapsed to take into account the Grace Period
- Once the validity status of the certificate is verified against the corresponding OCSP or CRL services taking into account the (trusted) time reference and the Grace Period,
- The content of the claimed QC certificate supporting the received signature is further checked for presence of QcCompliance statement, QCP OID, the QcSSCD statement, or the QCP+ OID (as defined in ETSI TS 101 456 and ETSI TS 101 862),
- The issuer of the QC is searched in the corresponding Trusted List through the Compiled List. The applicable Trusted List should be the one from the Member State in which the Issuing CA is established or if it is not established in a Member State, the one from the Member State in which the Issuing CA service has been accredited .
- Once found the corresponding service entry in the applicable Trusted List should be further analysed with regards to the "Sti:Sie:aSi" information, the "Sie:Q" information and the current (or historical) status value ***for assessing whether or not the received signature is a QES or $AdES_{QC}$ or not***.

3 Using Trusted Lists to validate $AdES_{QC}$ and QES

3.1 Reference Verification Process of a Certificate against a Trusted List

The following reference verification process of a certificate against a Trusted List, depicted in Figure 4 below, has been initially developed during the Face-to-Face meeting organised by ETSI and the European Commission in the context of the TSL PlugTest facilities and event.

The interface to the reference verification process is the End-Entity Certificate, the Issuer and a point in time (defaults to current time) against which the verification should be processed.

The inputs to the reference verification process are:

- The End-Entity Certificate (X509[n]) or, if available, the chain of Certificates (**X509[]**) from the End-Entity Certificate up to some appropriate Trust Anchor according to the relying party's signature validation policy and being the result of previous steps of a complete electronic signature verification.

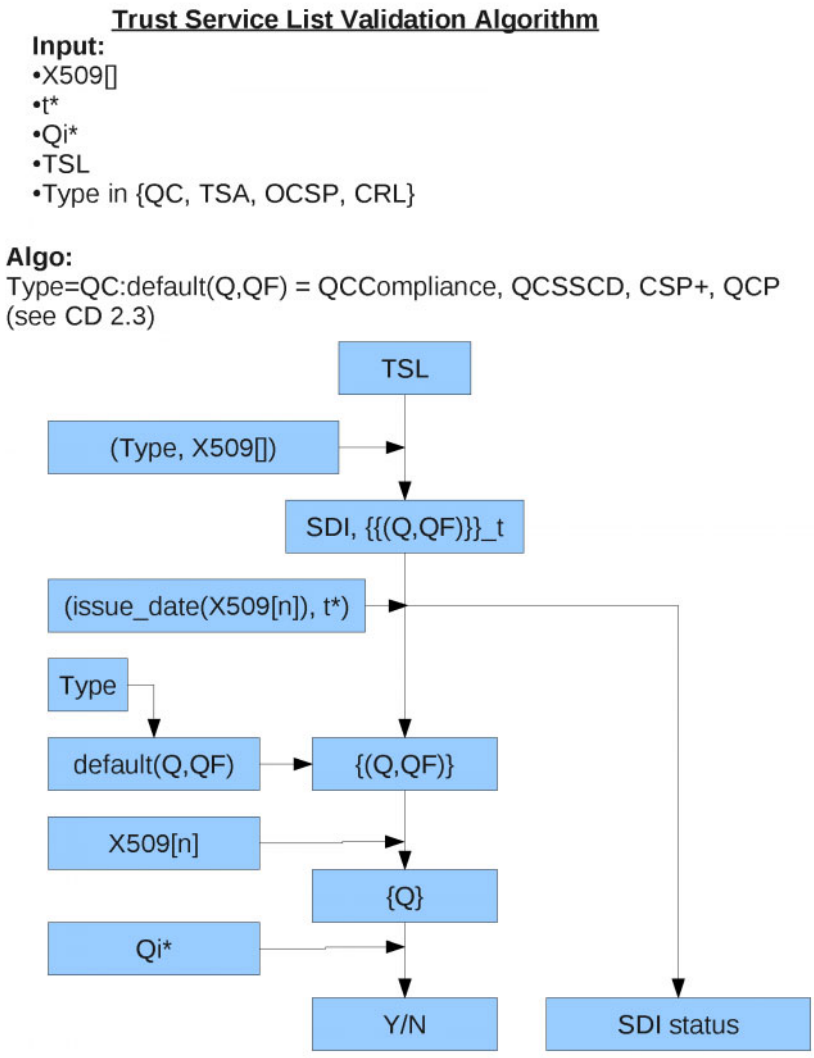
- An optional point in time (**t***) against which the verification should be processed. This allows for supplying the issue time of a CRL, the signing time of an OCSP response or to allow for the shell model. If not provided the date of issuance of the End-Entity Certificate (**issue_date(X509[n]**) is significant.

- An optional set of expected qualification statements (**Qi***). This allows to configure the verification process to check whether the End-Entity Certificate is a QC (QcCompliance statement, QCP certificate policy OID), whether the associated private key resides in an SSCD (QcSSCD statement, QCP+ certificate policy OID), or both.

- A **Trusted List** (preferably under a machine processable TSL implementation) or a set of them. The collection point for Trusted Lists is the European Commission **Compiled List** that should be used as a protected and trustworthy source of information for locating Member States national Trusted List and obtaining signature verification certificate to be sued to verify signed Trusted Lists.[26]

- The **Type of service** being one of {QC, TSA, OCSP, CRL} needed to be able to provide a default set of qualification statements according to CD 2009/767/EC and to discriminate the exceptional case where a certificate of the input chain (single “Sdi”) or one of its children is potentially used to provide services of different types.

[26] The country code found in the country (C) information as part of the Distinguished Name (DN) of the End-Entity Certificate Issuer should indicate the Member State in which the Issuing CA service is expected to be supervised. The same Issuing CA can be accredited as well in another Member State or, when not established in a Member State, may be accredited in any Member State.



(Source ETSI-Member States TSL interoperability face-to-face meeting Dec. 2009)

Figure 4

The conduction of the verification process towards the verification output can be described as follows:

- The TSL implementation of the applicable Trusted List is searched and provided as first step.
    - When the CA having issued the End-Entity certificate is established in a Member State[27] (country identification can be done through the Issuer Country name being part of the certificate information), the applicable Trusted List is expected to be the one from this identified country as this Member State is in charge of supervising the Issuing CA service. Note that in addition this Issuing CA may also be accredited in another Member State and hence be listed accordingly in this Member State's Trusted List.

[27] Or EEA country.

- When the CA having issued the End-Entity certificate is not established in a Member State, the applicable Trusted List is expected to be any one of the Member States Trusted List as any Member State may be in charge of accrediting such a Third Country Issuing CA service.

- The TSL is searched/filtered by Type and certificate chain and should only discover one "Service digital identity" (SDI) for a given Type.[28]

- This SDI, as being part of a listed certification service entry in the TSL, is associated to its current status ("Service current status") and its past statuses (in the "Service approval history", when not empty). It is also potentially associated with specific "Service information extensions" (SIEs) that:

    - In the "Qualifications" extension ("Sie:Q") may comprise of a set of tuples of qualifiers Q and filters QF written as {(Q,QF)} that may change over time _t along the service history written as {{(Q,QF)}}_t.

    - In the "additional Service Information" extension ("Sie:aSI") may comprise additional relevant information

    - In the "TakenOverBy" extension ("Sie:TOB") may comprise information on the legal entity having taken over the listed certification service when applicable.

- The right set is then selected at checking time **t*** if provided or otherwise at the date of issuance of the End-Entity Certificate (issue_date(X509[n]).

- [6], amended by [7], asks for the provision of default qualifiers depending on the type. In practice the matching of the filters QF with the End-Entity Certificate (X509[n]) should result in an external set or qualifiers {Q}. The union of this external set and the qualifiers within the certificate should return the right set of qualifiers if Scheme operators stick to the recommendations in [6][7].

- This resulting set of qualifiers is then compared with the set of expected qualification statements (**Qi***) that was provided as input before displaying accordingly the result of the verification process and the full and clear information about the "Sdi" status.

One should stress the importance of the nature and quality of the verification output display to the relying party. A simple answer yes/no or Green/Red is certainly not sufficient as the relying party is entitled to receive full and clear information about:

- Whether or not the End-Entity is a QC
- Whether or not the End-Entity private key associated to the certified public key resides in an SSCD
- What is the Issuing certification service supervision/accreditation status associated to the input point in time (t*) against which the verification process has been conducted
- What is the Issuing certification service supervision/accreditation status history
- What are the relevant additional information that should be taken into account from the certification service entry as listed in the Trusted List, namely information present in "Sie" and other relevant fields
- Access to additional information with regards to the certification service entry, certification service TSP, the Trusted List.

[28] Note that the type information of a listed service may be completed by the information, if any and if applicable, available in the "additionalServiceInformation" extension of the "Service information extensions" field (e.g. this may be used by some CSP to list a Root-CA certificate instead of dozens of subordinate Issuing CAs, see [6][7] specifications).

3.2 Existing tools

Few implementations of applications validating QC against a Trusted List have been developed so far, to our knowledge, and implementing fully the concept of QC validation against a Trusted List.

One must however notice the application developed in the context of activities within the Swedish single point of contact looking at practical implications of using TSL[29].

This application however took the option:

- To upload the TSL implementations of all Trusted List available from the European Commission Compiled List
- To provide a (very nice) interface to the viewing of all Trusted Lists, listed TSPs, and listed services, with sometimes interesting statistics
- To convert all Trusted Lists certification services information into a on-the-fly generated Cross-certification PKI hierarchy from an application local Root CA on the basis of validation policies that can be configured by the verifier.
    - This leads to some equivalent to a CA certificate Trust Store that can be understood as such by off-the-shelf applications like Adode Acrobat Reader and alike for trusting CAs
    - Configuration interface allows verifiers to create such trust Store to consider, e.g.:
        - Only CAs issuing QCs and that are accredited ,
        - Only CAs issuing QCs and that are in one of a valid supervision or accreditation status,
        - Any CA services issuing certificates and that are supervised
        - Etc.

While this application shows that Trusted Lists are available for use today and quite easy to manipulate to achieve such an impressive result, there are some warnings that are important to stress:

- Trusted Lists are much more than CA certificate Trust Stores as explained in previous sections of the present report, even when only considering certification services issuing QCs.

- The application does not consider, so far,

    - The content of the End-Entity Certificate in the validation process, at least not in a consolidated way when the verifier is willing to be convinced whether or not the received electronic signature is a QES or an $AdES_{QC}$ or not.

    - Important information provided in Trusted Lists to compensate the lack of information in QC with regards to the qualified statement or the support by an SSCD. This, as in the case of the Belgian example, may lead to trust issuing CA and mislead the verifier to validate the signature as a QES while the Trusted List confirms that the lack of information in the QC should be interpreted as not being supported by an SSCD.

- There is no need for any cross-certifying process in order to be able to use Trusted Lists. The approach used by the Swedish application is the quickest, while not complete or sufficient, when the goal is to integrate Trusted List usage in today's off-the-shelf application like Adobe Acrobat Reader, taking into account however all the concerns and limitations expressed in the present section.

However, liaison has been established with the designer of the Swedish application and further improvements may be expected in a near future.

In a similar approach, in order to conciliate classic X.509 certificate (path) validation implementations with the usage of Trusted Lists when assessing whether or not a received signature is a QES (or

[29] The slides and the presentation video are available from: http://aaa-sec.com/tsltrust/.

$AdES_{QC}$), and taking into account the fact that Trusted Lists are much more than Trust Stores, it might be possible to:

1. Consider the listed CA/QC "Sdi" certificates as "Trust Anchors" in a classic X.509 certificate (path) validation; build a regular chain of cryptographic dependency between the end-entity signer certificate considered and any of the listed CA/QC. No policy compatibility checking should be attempted to restrict the validity of this chaining, but standard X509 revocation checking applies. All CRLs and services involved should nevertheless also find a "Trust Anchor" amongst the listed accompanying services for this verification step to yield positive when applicable.

2. The Trusted List entry of the matching CA/QC service is used together with the signer's certificate content to assess whether it is a QC and whether it is supported by an SSCD, e.g. applying the reference verification process of a certificate against a Trusted List as described in section 3.1.

4 Conclusions and recommendations

The purpose of Trusted Lists (as defined in [6] [7]) is to provide the status of the listed services or more precisely of "the Common Template for Member States' 'Trusted List of supervised/accredited Certification Service Providers", thus establishing 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 (CSPs) who are supervised/ accredited by them, notably 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) 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).

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) supported by a Qualified Certificate.

Trusted Lists are significantly different from CA Certificate Trust Stores in terms of nature but also in terms of usage and they should be used accordingly. The above reference verification process of certificate against a Trusted List should be further developed, detailed and implemented in references applications, in particular in the context of the execution of the European Commission standardisation Mandate M460 [8].

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"[30].

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) [31],
- 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

[30] 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".

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

issuance and use of QC in Member States[32]. 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[33], 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};

[32] 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.

[33] 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[34]) 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

[34] 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.