Draft ETSI TS 119 615 V0.0.9 (2019-07)

Electronic Signatures and Infrastructures (ESI); Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists

Reference
DTS/ESI-0019615

Keywords
e-commerce, electronic signature, security,
trust services, EU qualified

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx.

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definition of terms, symbols, abbreviations and notations 7
3.1 Terms 7
3.2 Symbols 7
3.3 Abbreviations 7
3.4 Notations 7
4 Procedures for using and interpreting European Union Member States national trusted lists 8
4.0 General provisions 8
4.1 Authenticating the EC compiled list of trusted lists 8
4.1.1 Description 8
4.1.2 Inputs 9
4.1.3 Outputs 10
4.1.4 Processing 10
4.2 Authenticating a EUMS trusted list 12
4.2.1 Description 12
4.2.2 Inputs 12
4.2.3 Outputs 12
4.2.4 Processing 13
4.3 Obtaining certificate matching trust anchor service(s) 14
4.3.1 Description 14
4.3.2 Inputs 14
4.3.3 Outputs 14
4.3.4 Processing 14
4.4 EU qualified certificate determination 16
4.4.1 Description 16
4.4.2 Inputs 16
4.4.3 Outputs 16
4.4.4 Processing 17
4.5 QSCD determination 27
4.5.1 Description 27
4.5.2 Inputs 27
4.5.3 Outputs 27
4.5.4 Processing 28
4.6 EU qualified time stamp determination 30
4.6.1 Description 30
4.6.2 Inputs 30
4.6.3 Outputs 30
4.6.4 Processing 30
4.7 EU qualified validation service determination 32
4.7.1 Description 32
4.7.2 Inputs 32
4.7.3 Outputs 32
4.7.4 Processing 33
4.8 EU qualified preservation service determination 34
4.8.1 Description 34
4.8.2 Inputs 34
4.8.3 Outputs 35

4.8.4 Processing 35
4.9 EU qualified electronic registered delivery service determination 37
4.9.1 Description 37
4.9.2 Inputs and parameters 37
4.9.3 Outputs 37
4.9.4 Processing 38
History 40

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Trusted lists, as specified by ETSI TS 119 612 [1], enable in practice any interested party to determine whether a trust service is or was operating in compliance with relevant requirements, currently or at a given time in the past (e.g. at the time the service was provided, or at the time at which a transaction reliant on that service took place).

ETSI TS 119 612 [1] provides specifications supporting the establishment and management of trusted lists in two contexts, namely the European Union (EU) legislative context as set by Regulation (EU) No 910/2014 [i.1] and the context of countries outside the European Union and the EEA countries, or of international organizations willing to issue trusted lists in accordance with ETSI TS 119 612 [1].

The actual specifications for EU Member States (EUMS) national trusted lists are provided in Commission Implementing Decision (EU) 2015/1505 [i.2] laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 [i.1]. Those specifications and formats build upon ETSI TS 119 612 [1].

EUMS trusted lists have a legal constitutive value. It is the single formal source to verify that a claimed qualified trust service is indeed granted a qualified status by the competent EUMS body.

The rules for using and interpreting EUMS national trusted lists are provided in CID (EU) 2015/1505 [i.2]. The present document specifies procedures allowing for implementing those rules when validating EU qualified trust service outputs against such EUMS trusted lists (e.g. validating qualified certificates, EU qualified time stamps, evidences created by qualified electronic registered delivery services, EU electronic signatures or seals on EU qualified validation reports on EU qualified electronic signatures or seals).

1 Scope

The present document specifies procedures for using and interpreting EUMS national trusted lists when validating EU qualified trust service outputs against them (e.g. validating EU qualified certificates, EU qualified time stamps, evidences created by qualified electronic registered delivery services, EU electronic signatures or seals on EU qualified validation reports on EU qualified electronic signatures or seals).

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 119 612 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[2] ISO 3166-1:2013: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".

[3] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[i.2] Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D1505

[i.3] Official Journal of the European Union OJ C 233, 28.6.2016, p. 1–5. Information related to data on Member States' trusted lists as notified under Commission Decision 2009/767/EC, as amended by Decision 2010/425/EU and Implementing Decision 2013/662/EU and as notified under Implementing Decision (EU) 2015/1505.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.233.01.0001.01.ENG

[i.4] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardisation of signatures; Definitions and abbreviations".

[i.5] RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.6] RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[i.7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.8] RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[i.9] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.4] and the following apply:

pivot LOTL: specific instance of a LOTL that announces changes in the LOTL signing certificates and/or LOTL location

NOTE: Explanations on the concept of pivot LOTL can be found inhttps://youtu.be/J6LRcCx_yn0.

tuple: group of multiple elements or groups of multiple elements

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 119 001 [i.4] and the following apply:

EUMS	European Union Member State
LOTL	List Of Trusted Lists
LOTLSO	LOTL Scheme Operator
OJEU	Official Journal of the European Union
QTS	Qualified Trust Service
TL	Trusted List

3.4 Notations

The requirements in the present document are identified as follows:

<3 letters identifying the section title or type of requirement>-<the clause number>-<2-digit number (incremental)>

The management of the requirement identifiers for subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2-digits number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish new requirements.
- The requirement identifier for deleted requirements are kept and completed with "VOID".

- The requirement identifier for modified requirement are kept void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

4 Procedures for using and interpreting European Union Member States national trusted lists

4.0 General provisions

The present document presents procedures for using and interpreting European Union Member States national trusted lists in the form of algorithms, which provide a conformant behaviour when implemented by a conformant application.

GPR-4.0-01: Alternative implementations may be used provided that they shall produce the same output and main status indication when given the same set of input information.

GPR-4.0-02: The following parameters shall be preconfigured as follows for use in all the procedures specified in the remaining clauses of the present document:

Name	Description - Value
`OJEU-Loc`	URI value as appearing in the 'Scheme information URI' field of the LOTL (see clause 5.3.7 of ETSI TS 119 612 [1]) and referencing the latest publication of the OJEU related to data on EUMS TL as they are notified under Commission Implementing Decision (EU) 2015/1505 [i.2].
`LOTL-Loc`	URI value representing the location where the current instance of the XML file of the LOTL is available, as specified in the OJEU publication available from `OJEU-Loc`.
`LOTL-OJEU-Certs-Set`	The full set of certificates used for ensuring authenticity and integrity of the LOTL as provided in the OJEU publication available from `OJEU-Loc`.

NOTE 1: At the time of publication of the present document, the URI value described in the `OJEU-Loc` row of the above table was:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.233.01.0001.01.ENG

NOTE 2: Such configurations are likely to be performed outside the software application implementing the procedures specified in the present document and come from configuration files or other appropriate source.

GPR-4.0-03: In the procedures specified in the present document, whenever the validation of an https connection fails, implementations should refrain from stopping the processing for that reason but should add an appropriate warning to the corresponding procedure sub-status information.

4.1 Authenticating the EC compiled list of trusted lists

4.1.1 Description

EUMS trusted lists (TLs) have a legal constitutive value. It is the single formal source to verify that a claimed EU qualified trust service provider and the claimed EU qualified trust service it provides are indeed granted an EU qualified status by the competent EUMS body.

Regulation (EU) No 910/2014 [i.1] mandates EUMS to set up their national TL, at least under an XML machine processable format, compliant to the specifications established by CID (EU) 2015/1505 [i.2] building upon ETSI TS 119 612 [1].

EUMS have the obligation to electronically sign or seal the XML version of their national TL by means of a digital signature compliant with the specifications of CID (EU) 2015/1505 [i.2] relying on clause 5.7.1 of ETSI TS 119 612 [1]. To verify such a digital signature, relying parties need to be able to access the applicable public key.

In order to allow access to the TLs of all Member States in an easy manner, the European Commission (EC) publishes a central list, called the list of trusted lists (LOTL), with links to the locations where the TLs are published as notified by Member States. The public key certificate(s) corresponding to the private key(s) entitled to be used to sign EUMS TLs and hence to be used by relying parties to validate those TL signatures are notified by the EUMSs to the EC and published in the LOTL as well. The LOTL is available in a format suitable for automated processing (XML).

The authenticity and integrity of the machine processable version of the LOTL is ensured through a digital signature supported by a certificate which can be authenticated through a publication in the Official Journal of the European Union.

At the time of publication of the present document, pursuant to a publication in the Official Journal of the European Union (OJEU) C 233 [i.3], the LOTL can be accessed from the following location: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml.

OJEU C233 [i.3] additionally identifies and authenticates the LOTL scheme operator (LOTLSO) public key certificate(s) corresponding to the private key(s) entitled to be used to sign the LOTL and hence the public keys to be used by relying parties to validate the LOTL signature.

Both the location of the LOTL and the LOTLSO certificates can be updated through a new publication in the OJEU or through the mechanism of pivot LOTL in accordance with OJEU C233 [i.3]. The LOTLSO certificates and the location of the LOTL XML file are contained in the LOTL itself, as part of the first tuple of the 'Pointers to other TSLs' field of the LOTL as specified in clause 5.3.13 of ETSI TS 119 612 [1]. This enables relying parties to detect in a machine processable way a change in the LOTLSO certificates and/or in its location. Any such future change will be reflected in the publication of a new instance of a pivot LOTL which will include a new location URL and/or a modified set of digital certificates for relying parties to use when authenticating the LOTL. The change of the location of the LOTL will always lead to a new publication of the OJEU to authenticate such a new location. A change of the LOTL location is announced in a pivot LOTL while the previous location is maintained and the current instance of the LOTL is kept available at that location until the next publication in the OJEU.

Starting at the date of issuance of the pivot LOTL in which new LOTLSO certificates and/or new location is first published, the new URL and/or a modified set of digital certificates can be used by relying parties to locate and authenticate the LOTL in replacement of the formerly issued information. It is however always possible for the European Commission to publish a new publication in the OJEU, for instance as a temporary response to an emergency situation requiring the immediate replacement of all the digital certificates of the LOTL.

Each instance of the LOTL will include, as the first part of the information regarding the underlying scheme ('Scheme information URI" element as specified in clause 5.3.7 of ETSI TS 119 612 [1]), in their chronological order showing the most recent element first, the list of:

- One or more URLs where the last archived previous instance(s) of the pivot LOTL containing a new location and/or a modified set of digital certificates of the LOTL is(are) published, back until and followed by;
- The URL of the latest relevant publication in the OJEU resetting the initial location and the initial set of digital certificates for relying parties to use when authenticating the LOTL.

Each pivot LOTL is digitally signed by means of a private key for which the corresponding digital certificate is part of the set of LOTLSO certificates included in the previous pivot LOTL or included in the latest OJEU publication when the pivot LOTL is the first from that OJEU publication.

The current instance of the LOTL includes the exact same set of LOTLSO certificates included in the previous pivot LOTL and is digitally signed by means of a private key corresponding to one of these LOTLSO certificates.

The procedure specified in clause 4.1 allows to obtain the authenticated XML version of the current instance of the LOTL.

4.1.2 Inputs

Void.

4.1.3 Outputs

Name	Description
Authenticated-LOTL	The authenticated XML version of the current instance of the LOTL.
LOTL-Status	The status indication of the process of authenticating the current instance of the LOTL.
LOTL-Sub-Status	A list of indications supplementing LOTL-Status indication of the process of authenticating the current instance of the LOTL.

OUT-4.1.3-01: All above listed output variables shall be initialised to void.

4.1.4 Processing

NOTE: The processing basically checks the chain of trust between the LOTL XML file obtained from LOTL-Loc input and the LOTL-OJEU-Certs-Set input. It checks in particular that:

- The public key certificate corresponding to the private key having signed the LOTL XML file is part of the set of certificates included in the LOTL itself as part of the pointer to itself;
- When no pivot LOTL is present, the public key certificate corresponding to the private key having signed the LOTL XML file is part of the set of certificates included in the LOTL-OJEU-Certs-Set.
- When pivot LOTL is/are present:
  - Each pivot LOTL is signed by means of a private key for which the corresponding digital certificate:
    - is part of the set of certificates included in the previous pivot LOTL or included in the latest OJEU publication when the pivot LOTL is the first from that OJEU publication; and
    - is part of the set of certificates included in the pivot LOTL itself as part of the pointer to itself;
  - The current instance of the LOTL includes the exact same set of LOTLSO certificates included in the previous pivot LOTL and is signed by means of a private key corresponding to one of these LOTLSO certificates.
- The signatures of the LOTL and of each pivot LOTL are valid.

Additional consistency checks are performed.

PRO-4.1.4-01: The processing shall set LOTL to the current instance of the LOTL XML file obtained from LOTL-Loc.

PRO-4.1.4-02: The processing shall set LOTL-Signer-Cert to the ds:X509Certificate value of the ds:KeyInfo of the ds:Signature of LOTL.

PRO-4.1.4-03: The processing shall set 'n' to the number of consecutive URIs having an https scheme, an authority, and a non-empty path ending with the character string ".xml" as they are listed in the 'Scheme information URI' element of LOTL as specified in clause 5.3.7 of ETSI TS 119 612 [1].

PRO-4.1.4-04: If the n+1th URI of the 'Scheme information URI' element of LOTL as specified in clause 5.3.7 of ETSI TS 119 612 [1] is not matching OJEU-Loc then:

(a) The processing shall set Authenticated-LOTL to void,
(b) The processing shall set LOTL-Status to the value "LOTL_VERIFICATION_FAILED",
(c) The processing shall set LOTL-Sub-Status to the value "OJEU_LOCATION_INPUT_NOT_MATCHING_OJEU_LOCATION_IN_LOTL", and
(d) The processing shall stop the process.

PRO-4.1.4-05: If LOTL-Loc is not matching the TSLLocation string available in the tuple from the 'Pointers to other TSLs' field of LOTL (see clause 5.3.13 of ETSI TS 119 612 [1]) whose 'Scheme territory' qualifier has the value "EU" and if LOTL does not match the XML file obtained from that TSLLocation string, then:

(a) The processing shall set Authenticated-LOTL to void,
(b) The processing shall set LOTL-Status to the value "LOTL_VERIFICATION_FAILED",
(c) The processing shall set LOTL-Sub-Status to the value "LOTL_FILE_CONFLICT", and
(d) The processing shall stop the process.

PRO-4.1.4-06: If LOTL-Loc is matching the TSLLocation string available in the tuple from the 'Pointers to other TSLs' field of LOTL (see clause 5.3.13 of ETSI TS 119 612 [1]) whose 'Scheme territory' qualifier has the value "EU" and if LOTL does not match the XML file obtained from that TSLLocation string, then:

(a) The processing shall set LOTL to the XML file obtained from that TSLLocation string, and
(b) The processing shall go to PRO-4.1.4-02.

NOTE: This case corresponds to the publication of a new LOTL instance from the time of the initialisation of LOTL.

PRO-4.1.4-07: The processing shall validate ds:Signature of LOTL considering LOTL-Signer-Cert as a directly trusted certificate, i.e. as a trust anchor.

NOTE: This corresponds to the basic signature validation process of EN 319 102-1 [i.9].

PRO-4.1.4-08: If the signature validation performed in PRO-4.1.4-07 failed or was indeterminate, then:

a. The processing shall set Authenticated-LOTL to void,
b. The processing shall set LOTL-Status to the value "LOTL_VERIFICATION_FAILED",
c. The processing shall set LOTL-Sub-Status to the values provided by the validation procedure together with the additional value "LOTL_SIGNATURE_VERIFICATION_FAILED", and
d. The processing shall stop the process.

PRO-4.1.4-09: The processing shall set the following variables to the following values:

(a) LOTLSO-Cert to LOTL-Signer-Cert, and
(b) LOTLSO-Certs-Set to the full set of certificates available in the tuple from the 'Pointers to other TSLs' field (see clause 5.3.13 of ETSI TS 119 612 [1]) of LOTL, whose 'Scheme territory' qualifier has the value "EU".

PRO-4.1.4-10: If n is equal to 0, then

(a) If LOTL-Cert is not part of LOTLSO-Certs-Set then:
    a. The processing shall set Authenticated-LOTL to void,
    b. The processing shall set LOTL-Status to the value "LOTL_VERIFICATION_FAILED",
    c. The processing shall set LOTL-Sub-Status to the value "LOTL_SIGNER_CERT_NOT_AUTHENTICATED_BY_LOTL", and
    d. The processing shall stop the process.
(b) The processing shall go to PRO-4.1.4-12.

PRO-4.1.4-11: For all i in [1..n]

(a) The processing shall set Pivot to the instance of the XML file obtained from the i^{th} URI in the 'Scheme information URI" (see clause 5.3.7 of ETSI TS 119 612 [1]) field of LOTL having an https scheme, an authority, and a non-empty path ending with the character string ".xml", considering the first such URI as number 1.
(b) The processing shall set LOTLSO-Certs-Set to the full set of certificates as they are available in the tuple from the 'Pointers to other TSLs' field (see clause 5.3.13 of ETSI TS 119 612 [1]) of Pivot, whose 'Scheme territory' qualifier has the value "EU".
(c) If LOTLSO-Cert is not part of LOTLSO-Certs-Set then:
    a. The processing shall set Authenticated-LOTL to void,
    b. The processing shall set LOTL-Status to the value "LOTL_VERIFICATION_FAILED",

c. The processing shall set LOTL-Sub-Status to the value "PIVOT_i-1_SIGNER_CERT_NOT_AUTHENTICATED_BY_PIVOT_i", and
d. The processing shall stop the process.

(d) The processing shall set LOTLSO-Cert to the ds:X509Certificate value of the ds:KeyInfo of the ds:Signature of Pivot.

(e) The processing shall validate ds:Signature of Pivot considering LOTLSO-Cert as a directly trusted certificate, i.e. as a trust anchor.

NOTE: This corresponds to the basic signature validation process of EN 319 102-1 [i.9].

(f) If the signature validation performed in the previous point failed or was indeterminate then:
a. The processing shall set Authenticated-LOTL to void,
b. The processing shall set LOTL-Status to the value "LOTL_VERIFICATION_FAILED",
c. The processing shall set LOTL-Sub-Status to the values provided by the validation procedure together with the additional value "PIVOT_i_SIGNATURE_VERIFICATION_FAILED", and
d. The processing shall stop the process.

(g) If LOTLSO-Cert is not part of LOTLSO-Certs-Set then:
a. The processing shall set Authenticated-LOTL to void,
b. The processing shall set LOTL-Status to the value "LOTL_VERIFICATION_FAILED",
c. The processing shall set LOTL-Sub-Status to the value "PIVOT_i_SIGNER_CERT_NOT_AUTHENTICATED_BY_PIVOT_i", and
d. The processing shall stop the process.

PRO-4.1.4-12: If LOTLSO-Cert is not part of LOTL-OJEU-Certs-Set then:

a. The processing shall set Authenticated-LOTL to void,
b. The processing shall set LOTL-Status to the value "LOTL_VERIFICATION_FAILED",
c. The processing shall set LOTL-Sub-Status to the value "PIVOT_n_LOTLSO_SIGNER_CERT_NOT_AUTHENTICATED_BY_OJEU", and
d. The processing shall stop the process.

PRO-4.1.4-13: If the 'Next update' date of LOTL (see clause 5.3.15 of ETSI TS 119 612 [1]) has passed then the processing shall add to LOTL-Sub-Status the value "WARNING_LOTL_NEXTUPDATE_PASSED".

PRO-4.1.4-14: The processing shall set Authenticated-LOTL to LOTL.

PRO-4.1.4-15: The processing shall set LOTL-Status to the value "LOTL_VERIFICATION_PASSED".

4.2 Authenticating a EUMS trusted list

4.2.1 Description

The procedure specified in clause 4.2 allows to obtain the authenticated XML version of the national TL of a given EUMS.

4.2.2 Inputs

Name	Description
CC	Country code of the EUMS for which the trusted list is to be authenticated and whose value is in accordance with the ISO 3166-1 [2] Alpha 2 country code, set in capital letters.

4.2.3 Outputs

Name	Description
Authenticated-EUTL	The authenticated XML version of the requested TL of EUMS CC.

EUTL-Status	The status indication of the process of authenticating the requested TL of EUMS CC.
EUTL-Sub-Status	A list of indications supplementing EUTL-Status indication of the process of authenticating the requested TL of EUMS CC.

OUT-4.2.3-01: All above listed output variables shall be initialised to void.

4.2.4 Processing

PRO-4.2.4-01: The processing shall run the process for authenticating the LOTL as described in clause 4.1 of the present document.

PRO-4.2.4-02: If the output Authenticated-LOTL is void as a result of the execution of the process referred in PRO-4.2.4-01, then:

(a) The processing shall set EUTL-Status to the value "TL_VERIFICATION_FAILED";
(b) The processing shall set EUTL-Sub-Status to the values provided by set of values from LOTL-Status and LOTL-Sub-Status; and
(c) The processing shall stop the process.

PRO-4.2.4-03: The processing shall set EUTL-Loc to the URI provided in the tuple from the 'Pointers to other TSLs' field of Authenticated-LOTL (see clause 5.3.13 of ETSI TS 119 612 [1]) for which the 'Scheme territory' qualifier has value CC and for which the 'MIME type' is XML.

PRO-4.2.4-04: The processing shall set EUTL to the XML file retrieved from EUTL-Loc.

PRO-4.2.4-05: The processing shall set EUTL-Certs-Set to the set of certificates provided in the tuple from the 'Pointers to other TSLs' field of Authenticated-LOTL (see clause 5.3.13 of ETSI TS 119 612 [1]) for which the 'Scheme territory' qualifier has value CC and for which the 'MIME type' is XML.

PRO-4.2.4-06: The processing shall set EUTL-Signer-Cert to the ds:X509Certificate value of the ds:KeyInfo of the ds:Signature of EUTL.

PRO-4.2.4-07: If EUTL-Signer-Cert is not part of EUTL-Certs-Set, then:

(a) The processing shall set Authenticated-EUTL to void,
(b) The processing shall set EUTL-Status to the value "EUTL_VERIFICATION_FAILED",
(c) The processing shall set EUTL-Sub-Status to the value "EUTLSO_SIGNER_CERT_NOT_AUTHENTICATED_BY_LOTL", and
(d) The processing shall stop the process.

PRO-4.2.4-08: The processing shall validate ds:Signature of EUTL considering EUTL-Signer-Cert as a directly trusted certificate, i.e. as a trust anchor.

PRO-4.2.4-09: If the signature validation performed in PRO-4.2.4-08 failed, then:

(a) The processing shall set Authenticated-EUTL to void,
(b) The processing shall set EUTL-Status to the value "EUTL_VERIFICATION_FAILED",
(c) The processing shall set EUTL-Sub-Status to the set of values provided by the validation procedure together with the value "EUTL_SIGNATURE_VERIFICATION_FAILED", and
(d) The processing shall stop the process.

PRO-4.2.4-10: If the 'Next update' date of EUTL (see clause 5.3.15 of ETSI TS 119 612 [1]) has passed, then the processing shall add to EUTL-Sub-Status the value "WARNING_EUTL_NEXTUPDATE_PASSED".

PRO-4.2.4-11: The processing shall set Authenticated-EUTL to EUTL.

PRO-4.2.4-12: The processing shall set EUTL-Status to the value "EUTL_VERIFICATION_PASSED".

4.3 Obtaining certificate matching trust anchor service(s)

4.3.1 Description

The procedure specified in clause 4.3 allows to obtain matching service trust anchors, associated service information for a certificate for a specific date and time, for a specific service type identifier.

NOTE: The difference between a QTS type and a Service type identifier as specified in clause 5.5.1.1 of ETSI TS 119 612 [1] may reside in the sub-definition of that identifier service type into sub-services defined through 'additionalServiceInformation' extensions (see clause 5.5.9.4 of ETSI TS 119 612 [1]).

4.3.2 Inputs

Name	Description
CERT	X.509 certificate for which the information is to be obtained (e.g. a ds:X509Certificate value of a ds:KeyInfo of the ds:Signature)
TLS-Sti	One of the Service type identifier URI values specified in clause 5.5.1.1 of ETSI TS 119 612 [1].
Date-time	Date and time indication as specified in clause 5.1.3 of ETSI TS 119 612 [1].
CC	Country code value in accordance with the ISO 3166-1 [2] Alpha 2 country code, set in capital letters.

4.3.3 Outputs

Name	Description
SI-Results	A set of groups of elements, each group made of: (a) SI-full defined as an XML section corresponding to a 'Service information' element as specified in clause 5.5 of ETSI TS 119 612 [1]; (b) SI-at-Date-time defined as an XML section corresponding either to the Date-time related 'Service (current) information' element as specified in clause 5.5 of ETSI TS 119 612 [1] with the exception of clause 5.5.10 or to the Date-time related 'Service history instance' element as specified in clause 5.6 of ETSI TS 119 612 [1]; (c) TSP-Name defined as a 'TSP name' element as defined in clause 5.4.1 of ETSI TS 119 612 [1]; and (d) TSP-Trade-Name defined as a 'TSP trade name' element as defined in clause 5.4.2 of ETSI TS 119 612 [1].
SI-Status	The status indication of the process consisting in obtaining for a certificate, for a specific type of 'Service type identifier' URI value specified in clause 5.5.1.1 of ETSI TS 119 612 [1] and for a specific date and time, a matching trust anchor service and its associated service information.
SI-Sub-Status	A list of indications supplementing SI-Status indication of the process.

OUT-4.3.3-01: All above listed output variables shall be initialised to void.

4.3.4 Processing

PRO-4.3.4-01: If CC represents an EUMS and/or is set to "GB" or "UK":

(a) Then the processing shall run the process for authenticating the EUMS trusted list from CC as described in clause 4.2 of the present document, passing CC as input to the process;
(b) Else:
    a. The processing shall set SI-Status to the value "PROCESS_FAILED";
    b. The processing shall set SI-Sub-Status to the value "Provided_country_code_not_representing_an_EU_MS"; and

c. The processing shall stop the process.

PRO-4.3.4-02: If the output `Authenticated-EUTL` is void as a result of the execution of the process referred in PRO-4.3.4-01, then:

(a) The processing shall set `SI-Status` to the value "PROCESS_FAILED";
(b) The processing shall set `SI-Sub-Status` to the values provided by set of values from `EUTL-Status` and `EUTL-Sub-Status`; and
(c) The processing shall stop the process.

PRO-4.3.4-03: Parsing the `Authenticated-EUTL`, for each 'Service information' entry (see clause 5.5 of ETSI TS 119 612 [1]) for which:

(i) the 'Service type identifier' (see clause 5.5.1 of ETSI TS 119 612 [1]) matches `TLS-Sti`, and

(ii) either a certification path (see RFC 5280 [i.5]) is found from the 'Service digital identity' public key to `CERT`, in which the `organizationName` attribute of the `subjectName` field of the certificate provided in 'Service digital identity' matches the `organizationName` attribute of the `issuerName` field of `CERT`;

or the 'Service digital identity' public key is identical to the public key in `CERT`,

the processing shall add a tuple to `SI-Results` with:

NOTE 1: In function of the `TLS-Sti` value, the length of the certification path can be "0", "1" or longer.

NOTE 2: Building the certification path, the above 'Service digital identity' public key is considered as trust anchor.

(a) `SI-full` set to the entire such 'Service information' entry (see clause 5.5 of ETSI TS 119 612 [1]), and
(b) `SI-at-Date-time` set to:
    a. Either the entire such 'Service information' entry excepted, if any, the 'Service history' element (see clause 5.5.10 of ETSI TS 119 612 [1]) when `Date-time` is greater than or equal to 'Current status starting date and time' of that entry (see clause 5.5.5 of ETSI TS 119 612 [1]),
    b. Or the first 'Service history instance' (see clause 5.6 of ETSI TS 119 612 [1]) of that entry for which the 'Previous status starting date and time' (see clause 5.6.5 of ETSI TS 119 612 [1]) is less than or equal to `Date-time`.
(c) `TSP-Name` set to the 'TSP name' element (see clause 5.4.1 of ETSI TS 119 612 [1]) associated to that 'Service information' entry; and
(d) `TSP-Trade-Name` set to the 'TSP trade name' element (see clause 5.4.2 of ETSI TS 119 612 [1]) associated to that 'Service information' entry.

PRO-4.3.4-04: The processing shall set `SI-Status` to the value "PROCESS_PASSED".

PRO-4.3.4-05: The processing shall add to `SI-Sub-Status` the indication value "WARNING_T1_DUPLICATION" when two or more of the `SI-Results` tuples include an `SI-at-Date-time` XML section for which:

(a) an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) includes the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures", and
(b) values included in the respective 'Service current status" and/or 'Service previous status' fields (see respectively clauses 5.5.4 and 5.6.4 of ETSI TS 119 612 [1]) are identical.

PRO-4.3.4-06: The processing shall add to `SI-Sub-Status` the indication value "ERROR_T1_DUPLICATION" when two or more of the `SI-Results` tuples include an `SI-at-Date-time` XML section for which:

(a) an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) includes the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures", and
(b) values included in the respective 'Service current status" and/or 'Service previous status' fields (see respectively clauses 5.5.4 and 5.6.4 of ETSI TS 119 612 [1]) are not identical.

PRO-4.3.4-07: The processing shall add to `SI-Sub-Status` the indication value "WARNING_T2_DUPLICATION" when two or more of the `SI-Results` tuples include an `SI-at-Date-time` XML section for which:

(a) an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) includes the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals", and
(b) values included in the respective 'Service current status" and/or 'Service previous status' fields (see respectively clauses 5.5.4 and 5.6.4 of ETSI TS 119 612 [1]) are identical.

PRO-4.3.4-08: The processing shall add to `SI-Sub-Status` the indication value "ERROR_T2_DUPLICATION" when two or more of the `SI-Results` tuples include an `SI-at-Date-time` XML section for which:

(a) an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) includes the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals", and
(b) values included in the respective 'Service current status" and/or 'Service previous status' fields (see respectively clauses 5.5.4 and 5.6.4 of ETSI TS 119 612 [1]) are not identical.

PRO-4.3.4-09: The processing shall add to `SI-Sub-Status` the indication value "WARNING_T3_DUPLICATION" when two or more of the `SI-Results` tuples include an `SI-at-Date-time` XML section for which:

(a) an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) includes the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication", and
(b) values included in the respective 'Service current status" and/or 'Service previous status' fields (see respectively clauses 5.5.4 and 5.6.4 of ETSI TS 119 612 [1]) are identical.

PRO-4.3.4-10: The processing shall add to `SI-Sub-Status` the indication value "ERROR_T3_DUPLICATION" when two or more of the `SI-Results` tuples include an `SI-at-Date-time` XML section for which:

(a) an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) includes the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication", and
(b) values included in the respective 'Service current status" and/or 'Service previous status' fields (see respectively clauses 5.5.4 and 5.6.4 of ETSI TS 119 612 [1]) are not identical.

PRO-4.3.4-11: When two or more of the `SI-Results` tuples include different `TSP-Name` values, then:

(a) The processing shall add to `SI-Sub-Status` the indication value "ERROR_TSP_CONFLICT"; and
(b) The processing shall set `SI-Status` to the value "PROCESS_FAILED".

4.4 EU qualified certificate determination

4.4.1 Description

The procedure specified in clause 4.4 allows determining whether a certificate is confirmed by the applicable EUMS trusted list to have been an EU qualified certificate at a specific date and time and for which type.

4.4.2 Inputs

Name	Description of inputs
`CERT`	X.509 certificate for which the information is to be obtained (e.g. a `ds:X509Certificate` value of a `ds:KeyInfo` of the `ds:Signature`)
`Date-time`	Date and time indication as specified in clause 5.1.3 of ETSI TS 119 612 [1].

4.4.3 Outputs

Name	Description
`QC-Results`	A set of indications of the EU qualified status of `CERT` through one or more of the following values: (a) "Not_Qualified" to indicate that `CERT` is not an EU qualified certificate according to the EUMS trusted list from `CC` at `Date-time;`

	(b) "Not_Qualified_For_eSig" to indicate that CERT is not an EU qualified certificate for electronic signatures according to the EUMS trusted list from CC at Date-time; (c) "Not_Qualified_For_eSeal" to indicate that CERT is not an EU qualified certificate for electronic seals according to the EUMS trusted list from CC at Date-time; (d) "Not_QWAC" to indicate that CERT is not an EU qualified certificate for website authentication according to the EUMS trusted list from CC at Date-time; (e) "QC_For_eSig" to indicate that CERT is an EU qualified certificate for electronic signatures according to the EUMS trusted list from CC at Date-time; (f) "QC_For_eSeal" to indicate that CERT is an EU qualified certificate for electronic seals according to the EUMS trusted list from CC at Date-time; (g) "QWAC" to indicate that CERT is an EU qualified certificate for web site authentication according to the EUMS trusted list from CC at Date-time; (h) "INDET_QC_For_eSig" to indicate that the EUMS trusted list from CC cannot be used to confirm that CERT is a qualified certificate for electronic signatures at Date-time; (i) "INDET_QC_For_eSeal" to indicate that the EUMS trusted list from CC cannot be used to confirm that CERT is a qualified certificate for electronic seals at Date-time; (j) "INDET_QWAC" to indicate that the EUMS trusted list from CC cannot be used to confirm that CERT is a qualified certificate for website authentication at Date-time; (k) "INDETERMINATE"; (l) Void.
QC-Status	The status indication of the process.
QC-Sub-Status	A list of indications supplementing QC-Status indication.
CHECK_1_SET-OF_QE	An intermediate result as defined in the process below
CHECK_2_SET-OF_QE	An intermediate result as defined in the process below
CHECK_3_SET-OF_QE	An intermediate result as defined in the process below

OUT-4.4.3-01: All above listed output variables shall be initialised to void.

4.4.4 Processing

PRO-4.4.4-01: The processing shall set CC to the country code value of the countryName attribute of the issuer field of the certificate provided in CERT, in capital letters in accordance with the ISO 3166-1 [2] Alpha 2 country code, with, when applicable:

(a) the country code value "GB" being converted to "UK";
(b) the country code value "GR" being converted to "EL".

PRO-4.4.4-02: The processing shall set TLS-Sti to the value "http://uri.etsi.org/TrstSvc/Svctype/CA/QC" as specified in clause 5.5.1.1 of ETSI TS 119 612 [1].

PRO-4.4.4-03: The processing shall run the process described in clause 4.3 of the present document, passing the following inputs to the process:

(a) CERT;

(b) TLS-Sti;

(c) Date-time;

(d) CC.

PRO-4.4.4-04: If the output SI-Status of the process run in PRO-4.4.4-03 has the value "PROCESS_FAILED", then:

(a) The processing shall set QC-Status to the value "PROCESS_FAILED";
(b) The processing shall set QC-Sub-Status to the values provided by set of values from SI-Status and SI-Sub-Status; and
(c) The processing shall stop the process.

PRO-4.4.4-05: If the output SI-Results of the process run in PRO-4.4.4-03 is void, then:

(a) The processing shall set QC-Status to the value "PROCESS_PASSED";
(b) The processing shall set QC-Sub-Status to the value "No_confirmation_found_in_EUMSTL_CC";
(c) The processing shall set QC-Results to the value "Not_Qualified"; and
(d) The processing shall stop the process.

PRO-4.4.4-06: If the organizationName attribute of the issuerName field of the certificate provided in CERT is not matching one of the values of TSP-Name or TSP-Trade-Name of the output SI-Results of the process run in PRO-4.4.4-03, then:

(a) The processing shall set QC-Status to the value "PROCESS_FAILED";
(b) The processing shall set QC-Results to the value "INDETERMINATE";
(c) The processing shall set QC-Sub-Status to the value "ERROR_TSP_NAME_INCONSISTENCY_BETWEEN_CERT_AND_TL"; and
(d) The processing shall stop the process.

PRO-4.4.4-07: When Date-time is before 2016-06-30T22:00:00Z, the processing shall go to PRO-4.4.4-33.

PRO-4.4.4-08: The processing shall set the working variable CHECK_1 to void.

NOTE: CHECK_1 is a variable defined as an indication whose possible values are the values present in Table 1.

PRO-4.4.4-09: If the output SI-Sub-Status of the process run in PRO-4.4.4-03 includes the value "ERROR_T1_DUPLICATION", then the processing shall set CHECK_1 to the value "INDET_QC_For_eSig" and shall go to PRO-4.4.4-16.

NOTE: The above check could also catch the "WARNING_T1_DUPLICATION" case and treat it the same way i.e. stopping the process and raising the warning. However, considering the trusted lists as legally constitutive information regarding the qualified status of a trust service and hence of one of its output (e.g. certificate, time stamp token, signed evidence), in the case the status information is consistent, the relying party can decide, despite the fact that such a construction of the trusted list is in conflict with CID (EU) 2015/1505 [i.2], to go further and still consider the information in the trusted list, provided no further inconsistency is discovered in the rest of the processing (e.g. conflicting service information qualifications extensions).

PRO-4.4.4-10: If the 'Service current status' or 'Service previous status' field of (any of) the SI-at-Date-time element(s) of the SI-Results tuples (from the process run in PRO-4.4.4-03) that include an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) having the value http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures, has the value "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn", then the processing shall set CHECK_1 to the value "Not_Qualified_For_eSig" and shall go to PRO-4.4.4-16.

PRO-4.4.4-11: The processing shall set CHECK_1_SET-OF_QE to the set of all 'QualificationElement' from all 'Qualifications' extensions (see clause 5.5.9.2 of ETSI TS 119 612 [1]) whose 'CriteriaList' element identifies CERT from all SI-at-Date-time elements of the SI-Results tuples (from the process run in PRO-4.4.4-03) that include an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) having the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures".

PRO-4.4.4-12: The processing shall proceed as follows:

(a) It shall identify the set of all applicable qualifiers as per the content of the 'Qualifier' descendant elements (see clause 5.5.9.2.3 of ETSI TS 119 612 [1]) of all 'QualificationElement' elements of CHECK_1_SET-OF_QE;

(b) In case one of the following qualifier or combinations is found, it shall set CHECK_1 to the value "INDET_QC_For_eSig", it shall add to QC-Sub-Status the value "WARNING_T1_TL_Inconsistency_in_applying_qualifiers", and it shall go to PRO-4.4.4-16:
   a. 'NotQualified' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified") and 'QCStatement' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement");
   b. 'QCForESig' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig") and 'QCForESeal' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal");
   c. 'QCForESig' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig") and 'QCForWSA' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA");
   d. 'QCForESeal' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal") and 'QCForWSA' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA"); or
   e. QCForLegalPerson ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForLegalPerson");

PRO-4.4.4-13: The processing shall get the information about the presence and content of the id-etsi-qcs-QcCompliance and id-etsi-qcs-QcType statements (see ETSI EN 319 412-5 [3], hereafter respectively QcCompliance and QcType) in CERT.

PRO-4.4.4-14: If it results from PRO-4.4.4-13 that CERT includes more than one QcType identifier in its QcType statement when present, then the processing shall add to QC-Sub-Status the value "WARNING_CERT_Inconsistency_in_QcType_qualifiers_Non-compliance_with_EN319412-5".

PRO-4.4.4-15: Using the applicable qualifiers identified in PRO-4.4.4-12.(a):

(a) The processing shall check whether the following qualifiers are present among them: 'QCForESig' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig"), 'NotQualified' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified") and 'QCStatement' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement");
(b) The processing shall use the information obtained in PRO-4.4.4-13 to select the appropriate row of Table 1, and shall use the information obtained in above point PRO-4.4.4-15.(a) to select the appropriate column of Table 1;

NOTE: Information in row1/column0 means, and corresponds to the case where, the QcCompliance statement is present in CERT without any QcType statement being present, or the QcCompliance statement is present in CERT together with QcType 1 statement. The meaning of the other rows of column0 can be deduced accordingly.

Information in row0/column1 means, and corresponds to the case where, none of the three qualifiers 'NotQualified', 'QCStatement', 'QCForESig' in the 'Qualifications' extensions (denoted Sie:Q in Table 1) applies to CERT. Information in row0/column5 means, and corresponds to the case where, both qualifiers 'QCStatement' and 'QCForESig' in the 'Qualifications' extensions (denoted Sie:Q in Table 1) apply to CERT. The meaning of the other columns of row0 can be deduced accordingly.

(c) The processing shall set CHECK_1 to the value found in the selected cell of Table 1;

EXAMPLE: If QcCompliance extension is present in CERT together with the QcType 3 and the qualifier 'QCForESig' applies to CERT as per the 'Qualifications' extension present in the PRO-4.4.4-13 matching SI-at-Date-time element, then the value set to CHECK_1 is "QC_For_eSig" (see row3/column4) .

(d) If row8/column3 of Table 1 was selected in step (b) above, then the processing shall add to QC-Sub-Status the value "WARNING_T1_Not_Enough_Info_on_QC_Type".

Table 1: QC-For-eSig determination

		Sie:aSI = ForeSignatures				
row0		None of Sie:Q NotQualified QCStatement QCForESig	Sie:Q NotQualified (with or without QCForESig)	Sie:Q QCStatement	Sie:Q QCForESig	Sie:Q QCStatement & QCForESig
row1	**QcCompliance or QcCompliance + QcType 1**	"QC_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"	"QC_For_eSig"	"QC_For_eSig"
row2	**QcCompliance + QcType 2**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"	"QC_For_eSig"
row3	**QcCompliance + QcType 3**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"	"QC_For_eSig"
row4	**QcCompliance + QcType 1 & QcType 2**	"INDET_QC_For_eSig"	"Not_Qualified_For_eSig"	"INDET_QC_For_eSig"	"QC_For_eSig"	"QC_For_eSig"
row5	**QcCompliance + QcType 1 & QcType 3**	"INDET_QC_For_eSig"	"Not_Qualified_For_eSig"	"INDET_QC_For_eSig"	"QC_For_eSig"	"QC_For_eSig"
row6	**QcCompliance + QcType 2 & QcType 3**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"	"QC_For_eSig"
row7	**QcCompliance + QcType 1 & QcType 2 & QCType 3**	"INDET_QC_For_eSig"	"Not_Qualified_For_eSig"	"INDET_QC_For_eSig"	"QC_For_eSig"	"QC_For_eSig"
row8	**no QcCompliance and no QcType**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"INDET_QC_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row9	**no QcCompliance + QcType 1**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row10	**no QcCompliance + QcType 2**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row11	**no QcCompliance + QcType 3**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row12	**no QcCompliance + QcType 1 & QcType 2**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"INDET_QC_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row13	**no QcCompliance + QcType 1 & QcType 3**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"INDET_QC_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row14	**no QcCompliance + QcType 2 & QcType 3**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row15	**no QcCompliance + QcType 1 & QcType 2 & QCType 3**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"INDET_QC_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
	column0	column1	column2	column3	column4	column5

PRO-4.4.4-16: The processing shall set the working variable `CHECK_2` to void.

NOTE: `CHECK_2` is a variable defined as an indication whose possible values are the values present in Table 2.

PRO-4.4.4-17: If the output `SI-Sub-Status` of the process run in PRO-4.4.4-03 includes the value "ERROR_T2_DUPLICATION", then the processing shall set `CHECK_2` to the value "INDET_QC_For_eSeal" and shall go to PRO-4.4.4-24.

NOTE: The above check could also catch the "WARNING_T2_DUPLICATION" case and treat it the same way i.e. stopping the process and raising the warning. However, considering the trusted lists as legally constitutive information regarding the qualified status of a trust service and hence of one of its output (e.g. certificate, time stamp token, signed evidence), in the case the status information is consistent, the relying party can decide, despite the fact that such a construction of the trusted list is in conflict with CID (EU) 2015/1505 [i.2], to go further and still consider the information in the trusted list, provided no further inconsistency is discovered in the rest of the processing (e.g. conflicting service information qualifications extensions).

PRO-4.4.4-18: If the 'Service current status' or 'Service previous status' field of (any of) the SI-at-Date-time elements of the SI-Results tuples (from the process run in PRO-4.4.4-03) that include an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) having the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals", has the value "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn", then the processing shall set CHECK_2 to the value "Not_Qualified_For_eSeal" and shall go to PRO-4.4.4-24.

PRO-4.4.4-19: The processing shall set CHECK_2_SET-OF_QE to the set of all 'QualificationElement' from all 'Qualifications' extensions (see clause 5.5.9.2 of ETSI TS 119 612 [1]) whose 'CriteriaList' element identifies CERT from all SI-at-Date-time elements of the SI-Results tuples (from the process run in PRO-4.4.4-03) that include an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) having the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals".

PRO-4.4.4-20: The processing shall proceed as follows:

(a) It shall identify the set of all applicable qualifiers as per the content of the 'Qualifier' descendant elements (see clause 5.5.9.2.3 of ETSI TS 119 612 [1]) of all 'QualificationElement' elements of CHECK_2_SET-OF_QE;
(b) In case one of the following qualifier or combinations is found, it shall set CHECK_2 to the value "INDET_QC_For_eSeal", it shall add to QC-Sub-Status the value "WARNING_T2_TL_Inconsistency_in_applying_qualifiers", and it shall go to PRO-4.4.4-24:
    a. 'NotQualified' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified") and 'QCStatement' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement");
    b. 'QCForESig' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig") and 'QCForESeal' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal");
    c. 'QCForESig' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig") and 'QCForWSA' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA"); or
    d. 'QCForESeal' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal") and 'QCForWSA' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA");

PRO-4.4.4-21: The processing shall get the information about the presence and content of the QcCompliance and QcType statements (see ETSI EN 319 412-5 [3]) in CERT.

PRO-4.4.4-22: If it results from PRO-4.4.4-21 that CERT includes more than one QcType identifier in its QcType statement when present, then the processing shall add to QC-Sub-Status the value "WARNING_CERT_Inconsistency_in_QcType_qualifiers_Non-compliance_with_EN319412-5".

PRO-4.4.4-23: Using the applicable qualifiers identified in PRO-4.4.4-20.(a):

(a) The processing shall check whether the following qualifiers are present among them: 'QCForESeal' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal"), 'NotQualified' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified") and 'QCStatement' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement");
(b) The processing shall use the information obtained in PRO-4.4.4-21 to select the appropriate row of Table 2, and shall use the information obtained in above point PRO-4.4.4-23.(a) to select the appropriate column of Table 2;

NOTE: Information in row1/column0 means, and corresponds to the case where, the QcCompliance statement is present in CERT without any QcType statement being present, or the QcCompliance statement is present in CERT together with QcType 1 statement. The meaning of the other rows of column0 can be deduced accordingly.

Information in row0/column1 means, and corresponds to the case where, none of the three qualifiers 'NotQualified', 'QCStatement', 'QCForESeal' in the 'Qualifications' extensions (denoted Sie:Q in Table 2) applies to CERT. Information in row0/column5 means, and corresponds to the case where, both qualifiers 'QCStatement' and 'QCForESeal' in the 'Qualifications' extensions apply to CERT. The meaning of the other columns of row0 can be deduced accordingly.

(c) The processing shall set CHECK_2 to the value found in the selected cell of Table 2;

EXAMPLE: If QcCompliance extension is present in CERT together with the QcType 3 and the qualifier 'QCForESeal' applies to CERT as per the 'Qualifications' extension present in the PRO-4.4.4-21 matching SI-at-Date-time element, then the value set to CHECK_2 is "QC_For_eSeal" (see row3/column4) .

(d) If row8/column3 of Table 2 was selected in step (b) above, then the processing shall add to `QC-Sub-Status` the value "WARNING_T2_Not_Enough_Info_on_QC_Type".

Table 2: QC-For-eSeal determination

		Sie:aSI = ForeSeals				
row0		None of Sie:Q NotQualified QCStatement QCForESeal	Sie:Q NotQualified (with or without QCForESeal)	Sie:Q QCStatement	Sie:Q QCForESeal	Sie:Q QCStatement & QCForESeal
row1	**QcCompliance or QcCompliance + QcType 1**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"	"QC_For_eSeal"
row2	**QcCompliance + QcType 2**	"QC_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"	"QC_For_eSeal"	"QC_For_eSeal"
row3	**QcCompliance + QcType 3**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"	"QC_For_eSeal"
row4	**QcCompliance + QcType 1 & QcType 2**	"INDET_QC_For_eSeal"	"Not_Qualified_For_eSeal"	"INDET_QC_For_eSeal"	"QC_For_eSeal"	"QC_For_eSeal"
row5	**QcCompliance + QcType 1 & QcType 3**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"	"QC_For_eSeal"
row6	**QcCompliance + QcType 2 & QcType 3**	"INDET_QC_For_eSeal"	"Not_Qualified_For_eSeal"	"INDET_QC_For_eSeal"	"QC_For_eSeal"	"QC_For_eSeal"
row7	**QcCompliance + QcType 1 & QcType 2 & QCType 3**	"INDET_QC_For_eSeal"	"Not_Qualified_For_eSeal"	"INDET_QC_For_eSeal"	"QC_For_eSeal"	"QC_For_eSeal"
row8	**no QcCompliance and no QcType**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"INDET_QC_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"
row9	**no QcCompliance + QcType 1**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"
row10	**no QcCompliance + QcType 2**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"
row11	**no QcCompliance + QcType 3**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"
row12	**no QcCompliance + QcType 1 & QcType 2**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"INDET_QC_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"
row13	**no QcCompliance + QcType 1 & QcType 3**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"
row14	**no QcCompliance + QcType 2 & QcType 3**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"INDET_QC_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"
row15	**no QcCompliance + QcType 1 & QcType 2 & QCType 3**	"Not_Qualified_For_eSeal"	"Not_Qualified_For_eSeal"	"INDET_QC_For_eSeal"	"Not_Qualified_For_eSeal"	"QC_For_eSeal"
	column0	column1	column2	column3	column4	column5

PRO-4.4.4-24: The processing shall set the working variable `CHECK_3` to void.

NOTE: `CHECK_3` is a variable defined as an indication whose possible values are the values present in Table 3.

PRO-4.4.4-25: If the output `SI-Sub-Status` of the process run in PRO-4.4.4-03 includes the value "ERROR_T3_DUPLICATION", then the processing shall set `CHECK_3` to the value "INDET_QWAC" and shall go to PRO-4.4.4-32.

NOTE: The above check could also catch the "WARNING_T3_DUPLICATION" case and treat it the same way i.e. stopping the process and raising the warning. However, considering the trusted lists as legally constitutive information regarding the qualified status of a trust service and hence of one of its output (e.g. certificate, time stamp token, signed evidence), in the case the status information is consistent, the relying party can decide, despite the fact that such a construction of the trusted list is in conflict with CID (EU) 2015/1505 [i.2], to go further and still consider the information in the trusted list, provided no further inconsistency is discovered in the rest of the processing (e.g. conflicting service information qualifications extensions).

PRO-4.4.4-26: If the 'Service current status' or 'Service previous status' field of (any of) the `SI-at-Date-time` elements of the `SI-Results` tuples (from the process run in PRO-4.4.4-03) that include an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) having the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication", has the value "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn", then the processing shall set CHECK_3 to the value "Not_QWAC" and go to PRO-4.4.4-32.

PRO-4.4.4-27: The processing shall set `CHECK_3_SET-OF_QE` to the set of all 'QualificationElement' from all 'Qualifications' extensions (see clause 5.5.9.2 of ETSI TS 119 612 [1]) whose 'CriteriaList' element identifies `CERT` from all `SI-at-Date-time` elements of the `SI-Results` tuples (from the process run in PRO-4.4.4-03) that include an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) having the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication".

PRO-4.4.4-28: The processing shall proceed as follows:

(a) It shall identify the set of all applicable qualifiers as per the content of the 'Qualifier' descendant elements (see clause 5.5.9.2.3 of ETSI TS 119 612 [1]) of all 'QualificationElement' elements of `CHECK_3_SET-OF_QE`;
(b) In case one of the following qualifier or combinations is found, it shall set `CHECK_3` to the value "INDET_QWAC", it shall add to `QC-Sub-Status` the value "WARNING_T3_TL_Inconsistency_in_applying_qualifiers", and it shall go to PRO-4.4.4-32:
    a. 'NotQualified' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified") and 'QCStatement' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement");
    b. 'QCForESig' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig") and 'QCForESeal' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal");
    c. 'QCForESig' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig") and 'QCForWSA' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA"); or
    d. 'QCForESeal' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal") and 'QCForWSA' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA");

PRO-4.4.4-29: The processing shall get the information about the presence and content of the QcCompliance and QcType statements (see ETSI EN 319 412-5 [3]) in `CERT`.

PRO-4.4.4-30: If it results from PRO-4.4.4-29 that `CERT` includes more than one QcType identifier in its QcType statement when present, then the processing shall add to `QC-Sub-Status` the value "WARNING_CERT_Inconsistency_in_QcType_qualifiers_Non-compliance_with_EN319412-5".

PRO-4.4.4-31: Using the applicable qualifiers identified in PRO-4.4.4-28.(a):

(a) The processing shall check whether the following qualifiers are present among them: 'QCForWSA' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA"), 'NotQualified' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified") and 'QCStatement' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement");
(b) The processing shall use the information obtained in PRO-4.4.4-29 to select the appropriate row of Table 3, and it shall use the information obtained in above point PRO-4.4.4-31.(a) to select the appropriate column of Table 3;

NOTE: Information in row1/column0 means, and corresponds to the case where, the QcCompliance statement is present in `CERT` without any QcType statement being present, or the QcCompliance statement is present in `CERT` together with QcType 1 statement. The meaning of the other rows of column0 can be deduced accordingly.

Information in row0/column1 means, and corresponds to the case where, none of the three qualifiers 'NotQualified', 'QCStatement', 'QCForWSA' in the 'Qualifications' extensions (denoted Sie:Q in Table 3) applies to CERT. Information in row0/column5 means, and corresponds to the case where, both qualifiers 'QCStatement' and 'QCForWSA' in the 'Qualifications' extensions apply to CERT. The meaning of the other columns of row0 can be deduced accordingly.

(c) The processing shall set CHECK_3 to the value found in the selected cell of Table 3;

EXAMPLE: If QcCompliance extension is present in CERT together with the QcType 3 and the qualifier 'QCForWSA' applies to CERT as per the 'Qualifications' extension present in the PRO-4.4.4-29 matching SI-at-Date-time element, then the value set to CHECK_3 is "QWAC" (see row3/column4).

Table 3: QC-For-WebSiteAuthentication determination

		Sie:aSI = ForWebSiteAuthentication				
row0		None of Sie:Q NotQualified QCStatement QCForWSA	Sie:Q NotQualified (with or without QCForWSA)	Sie:Q QCStatement	Sie:Q QCForWSA	Sie:Q QCStatement & QCForWSA
row1	**QcCompliance or QcCompliance + QcType 1**	"Not_QWAC"	"Not_QWAC"	"Not_QWAC"	"QWAC"	"QWAC"
row2	**QcCompliance + QcType 2**	"Not_QWAC"	"Not_QWAC"	"Not_QWAC"	"QWAC"	"QWAC"
row3	**QcCompliance + QcType 3**	"QWAC"	"Not_QWAC"	"QWAC"	"QWAC"	"QWAC"
row4	**QcCompliance + QcType 1 & QcType 2**	"Not_QWAC"	"Not_QWAC"	"Not_QWAC"	"QWAC"	"QWAC"
row5	**QcCompliance + QcType 1 & QcType 3**	"INDET_QWAC"	"Not_QWAC"	"INDET_QWAC"	"QWAC"	"QWAC"
row6	**QcCompliance + QcType 2 & QcType 3**	"INDET_QWAC"	"Not_QWAC"	"INDET_QWAC"	"QWAC"	"QWAC"
row7	**QcCompliance + QcType 1 & QcType 2 & QCType 3**	"INDET_QWAC"	"Not_QWAC"	"INDET_QWAC"	"QWAC"	"QWAC"
row8	**no QcCompliance and no QcType**	"Not_QWAC"	"Not_QWAC"	"INDET_QWAC"	"Not_QWAC"	"QWAC"
row9	**no QcCompliance + QcType 1**	"Not_QWAC"	"Not_QWAC"	"Not_QWAC"	"Not_QWAC"	"QWAC"
row10	**no QcCompliance + QcType 2**	"Not_QWAC"	"Not_QWAC"	"Not_QWAC"	"Not_QWAC"	"QWAC"
row11	**no QcCompliance + QcType 3**	"Not_QWAC"	"Not_QWAC"	"QWAC"	"Not_QWAC"	"QWAC"
row12	**no QcCompliance + QcType 1 & QcType 2**	"Not_QWAC"	"Not_QWAC"	"Not_QWAC"	"Not_QWAC"	"QWAC"
row13	**no QcCompliance + QcType 1 & QcType 3**	"Not_QWAC"	"Not_QWAC"	"INDET_QWAC"	"Not_QWAC"	"QWAC"
row14	**no QcCompliance + QcType 2 & QcType 3**	"Not_QWAC"	"Not_QWAC"	"INDET_QWAC"	"Not_QWAC"	"QWAC"
row15	**no QcCompliance + QcType 1 & QcType 2 & QCType 3**	"Not_QWAC"	"Not_QWAC"	"INDET_QWAC"	"Not_QWAC"	"QWAC"
	column0	column1	column2	column3	column4	column5

(d) If row8/column3 of Table 3 was selected in step (b) above, then the processing shall add to QC-Sub-Status the value "WARNING_T3_Not_Enough_Info_on_QC_Type".

PRO-4.4.4-32: Compare two by two the values of CHECK_1, CHECK_2, and CHECK_3 on the basis of Table 4 as follows:

(a) When the comparison results in an "error" indication:
   a. The processing shall set `QC-Status` to the value "PROCESS_FAILED";
   b. The processing shall add to `QC-Sub-Status` appropriate values reflecting the problematic two by two combinations; and
   c. The processing shall stop the process.
(b) The processing shall set `QC-Status` to the value "PROCESS_PASSED";
(c) The processing shall set `QC-Results` to the set of indications provided in `CHECK_1`, in `CHECK_2`, and in `CHECK_3`;
(d) When the comparison results in one or more "warning" indications:
   a. The processing shall set `QC-Status` to the value "PROCESS_PASSED_WITH_WARNING";
   b. The processing shall add to `QC-Sub-Status` appropriate values reflecting the problematic two by two combinations.

Table 4: QC status check

2 by 2 combinations	"QC_For_eSig"	"Not_Qualified_For_eSig"	"INDET_QC_For_eSig"	"QC_For_eSeal"	"Not_Qualified_For_eSeal"	"INDET_QC_For_eSeal"	"QWAC"	"Not_QWAC"	"INDET_QWAC"
"QC_For_eSig"				error	ok	warning	error	ok	warning
"Not_Qualified_For_eSig"				ok	ok	warning	ok	ok	warning
"INDET_QC_For_eSig"				warning	warning	warning	warning	warning	warning
"QC_For_eSeal"	error	ok	warning				error	ok	warning
"Not_Qualified_For_eSeal"	ok	ok	warning				ok	ok	warning
"INDET_QC_For_eSeal"	warning	warning	warning				warning	warning	warning
"QWAC"	error	ok	warning	error	ok	warning			
"Not_QWAC"	ok	ok	warning	ok	ok	warning			
"INDET_QWAC"	warning	warning	warning	warning	warning	warning			

(e) The processing shall go to PRO-4.4.4-34.

PRO-4.4.4-33: Proceed as follows:

(a) The processing shall set `CHECK_2` to the value "Not_Qualified_For_eSeal";
(b) The processing shall set `CHECK_3` to the value "Not_QWAC";
(c) If there are two or more of the `SI-Results` tuples (from the process run in PRO-4.4.4-03) that include an `SI-at-Date-time` XML section for which the values included in the 'Service previous status' fields (see clause 5.6.4 of ETSI TS 119 612 [1]) are identical, then the processing shall add to `QC-Sub-Status` the indication value "WARNING_TL-SERVICE-ENTRY-SDI_DUPLICATION";
(d) If there are two or more of the `SI-Results` tuples that include an `SI-at-Date-time` XML section for which the values included in the 'Service previous status' fields (see clause 5.6.4 of ETSI TS 119 612 [1]) are not identical, then:
   a. The processing shall add to `QC-Sub-Status` the indication value "ERROR_TL-SERVICE-ENTRY-SDI_DUPLICATION_STATUS_CONFLICT";
   b. The processing shall set `QC-Status` to the value "PROCESS_FAILED";
   c. The processing shall stop the process.
(e) The processing shall set `CHECK_1` to void;
(f) If the 'Service previous status' field of (any of) the `SI-at-Date-time` element(s) of the `SI-Results` tuples has one of the values "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased", "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionrevoked", "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationceased", or "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationrevoked", then:
   a. The processing shall set `CHECK_1` to the value "Not_Qualified_For_eSig";
   b. The processing shall set `QC-Status` to the value "PROCESS_PASSED";

c. The processing shall stop the process.

(g) The processing shall set CHECK_1_SET-OF_QE to the set of all 'QualificationElement' from all 'Qualifications' extensions (see clause 5.5.9.2 of ETSI TS 119 612 [1]) whose 'CriteriaList' element identifies CERT from all SI-at-Date-time elements of the SI-Results tuples (from the process run in PRO-4.4.4-03).

(h) The processing shall proceed as follows:

a. It shall identify the set of all applicable qualifiers as per the content of the 'Qualifier' descendant elements (see clause 5.5.9.2.3 of ETSI TS 119 612 [1]) of all 'QualificationElement' elements of CHECK_1_SET-OF_QE;

b. In case the qualifier "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal", the qualifier "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA", and/or combination of the qualifiers "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified" and "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement" is/are found, then:

i. The processing shall set CHECK_1 to the value "INDET_QC_For_eSig",

ii. The processing shall add to QC-Sub-Status the value "ERROR_T1_TL_Inconsistency_in_applying_qualifiers",

iii. The processing shall set QC-Status to the value "PROCESS_FAILED";

iv. The processing shall stop the process.

(i) The processing shall get the information about the presence in CERT of the id-etsi-qcs-QcCompliance statement (see ETSI EN 319 412-5 [3]), the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID, and/or the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID;

(j) The processing shall use the applicable qualifiers identified in PRO-4.4.4-33.(h).a to select the appropriate column of Table 5, and shall use the information obtained in PRO-4.4.4-33.(i) to select the appropriate row of Table 5;

Table 5: QC-For-eSig determination under Directive 1999/93/EC [i.7]

		Sti = CA/QC		
row0		None of Sie:Q NotQualified QCStatement	Sie:Q NotQualified	Sie:Q QCStatement
row1	**QcCompliance**	"QC_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row2	**PolicyId QCP (qcp-public)**	"QC_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row3	**PolicyId QCP+ (qcp-public-with-sscd)**	"QC_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row4	**Any combination of QcCompliance, PolicyId QCP, PolicyId QCP+**	"QC_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
row5	**None**	"Not_Qualified_For_eSig"	"Not_Qualified_For_eSig"	"QC_For_eSig"
	column0	column1	column2	column3

NOTE: Information in row1/column0 means, and corresponds to the case where, the QcCompliance statement is present in CERT. The meaning of the other rows of column0 can be deduced accordingly. Information in row0/column1 means, and corresponds to the case where, none of the three qualifiers 'NotQualified', 'QCStatement', 'QCForESig' in the 'Qualifications' extensions (denoted Sie:Q in Table 5) applies to CERT. The meaning of the other columns of row0 can be deduced accordingly.

(k) The processing shall set CHECK_1 to the value found in the selected cell of Table 5;

(l) The processing shall set QC-Status to the value "PROCESS_PASSED";

(m) The processing shall set QC-Results to the set of indications provided in CHECK_1, in CHECK_2, and in CHECK_3.

PRO-4.4.4-34: The processing shall run the process described in clause 4.4 of the present document, until either PRO-4.4.4-32 step is completed or PRO-4.4.4-33 step is completed, passing the following inputs to the process:

(a) `CERT`;

(b) The date and time value of the `NotBeforeDate` field of `CERT`.

PRO-4.4.4-35: If the output `QC-Status` of the process run in PRO-4.4.4-34 has the value "PROCESS_FAILED", then:

(a) The processing shall set `QC-Status` to the value "PROCESS_FAILED";
(b) The processing shall add to `QC-Sub-Status` the values provided by set of values from `QC-Status` and `QC-Sub-Status` from the process run in PRO-4.4.4-34; and
(c) The processing shall stop the process.

PRO-4.4.4-36: The processing shall compare the values of `QC-Results` obtained after the first run of process 4.4 (with `Date-time` from the input) and after the second run of process 4.4 (with the `NotBeforeDate`):

(a) When the two results do not contain the exact same set of indications then:
    a. The processing shall set `QC-Status` to the value "PROCESS_FAILED";
    b. The processing shall add to `QC-Sub-Status` appropriate values reflecting the problematic comparison(s); and
    c. The processing shall stop the process.

NOTE: When `QC-Results` include either "QC_For_eSig", or "QC_For_eSeal" or "QWAC", then CERT can be considered, at `Date-time`, respectively as an EU qualified certificate for electronic signatures, an EU qualified certificate for electronic seals, or an EU qualified certificate for website authentication.

(b) When the comparison results in one or more "warning" indications:
    a. The processing shall set `QC-Status` to the value "PROCESS_PASSED_WITH_WARNING";
    b. The processing shall add to `QC-Sub-Status` appropriate values reflecting the problematic comparison(s).

4.5 QSCD determination

4.5.1 Description

The procedure specified in clause 4.5 allows determining whether an EU qualified certificate is confirmed by the applicable EUMS trusted list to have had its private key residing in a QSCD at a specific date and time.

NOTE: As the EUMS trusted list provides such information only for qualified certificates of a certain type, the process will first determine whether or not the certificate is a qualified certificate and for which type.

4.5.2 Inputs

Name	Description of inputs
`CERT`	X.509 certificate for which the information is to be obtained (e.g. a `ds:X509Certificate` value of a `ds:KeyInfo` of the `ds:Signature`)
`Date-time`	Date and time indication as specified in clause 5.1.3 of ETSI TS 119 612 [1].

4.5.3 Outputs

Name	Description
`QSCD-Results`	An indication on whether `CERT` had its private key residing in a QSCD in accordance with the trusted lists, through one of the following values:

	(a) "QSCD_YES" to indicate that CERT had its private key residing in a QSCD at Date-time according to the EUMS trusted list from CC; (b) "QSCD_NO" to indicate that CERT did not have its private key residing in a QSCD at Date-time according to the EUMS trusted list from CC; (c) "QSCD_INDETERMINATE" to indicate that the EUMS trusted list from CC cannot be used to confirm that CERT had its private key residing in a QSCD at Date-time; (d) Void.
QSCD-Status	The status indication of the process.
QSCD-Sub-Status	A list of indications supplementing QSCD-Status indication.

OUT-4.5.3-01: All above listed output variables shall be initialised to void.

4.5.4 Processing

PRO-4.5.4-01: The processing shall run the process described in clause 4.4 of the present document, passing the following inputs to the process:

(a) CERT;

(b) Date-time.

PRO-4.5.4-02: If the output QC-Status of the process run in PRO-4.5.4-01 has the value "PROCESS_FAILED", then:

(a) The processing shall set QSCD-Status to the value "PROCESS_FAILED";
(b) The processing shall set QSCD-Sub-Status to the values provided by set of values from QC-Status and QC-Sub-Status; and
(c) The processing shall stop the process.

PRO-4.5.4-03: When Date-time is strictly before 2016-06-30T22:00:00Z:

(a) If QC_Results includes the value "QC_For_eSig", then considering CHECK_1_SET-OF_QE as part of the outputs of the process run in PRO-4.5.4-01:
    a. The processing shall identify the set of all applicable qualifiers as per the content of the 'Qualifier' descendant elements (see clause 5.5.9.2.3 of ETSI TS 119 612 [1]) of all 'QualificationElement' elements of CHECK_1_SET-OF_QE, and shall check whether the following qualifiers are present among them: 'QCWithSSCD' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD"), 'QCNoSSCD' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoSSCD"), and 'QCSSCDStatusAsInCert' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCSSCDStatusAsInCert");
    b. In case one of the following combinations is found, the processing shall set QSCD-Results to the value "QSCD_INDETERMINATE", shall set QSCD-Status to the value "PROCESS_PASSED_WITH_WARNING", shall add to QSCD-Sub-Status the value "WARNING_Inconsistency_in_applying_qualifiers_for_SSCD_status", and shall stop the process:
        i. 'QCWithSSCD' and 'QCNoSSCD';
        ii. 'QCSSCDStatusAsInCert' and 'QCWithSSCD'
        iii. 'QCSSCDStatusAsInCert' and 'QCNoSSCD'.
    c. The processing shall identify the presence of the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID in the CertificatePolicies extension and the presence of the QcSSCD statement in the QCStatements extension (see ETSI EN 319 412-5 [3]) in CERT;
    d. The processing shall use the information obtained in above point PRO-4.5.4-03.(a).a. to select the appropriate column of Table 6, and shall use the information obtained in above point PRO-4.5.4-03.(a).c. to select the appropriate row of Table 6, and set QSCD-Results to the value found in the selected cell;

Table 6: QSCD status check (Directive regime)

Sie:Q / CERT	"QCWithSSCD"	"QCSSCDStatusAsInCert" or no indication	"QCNoSSCD"
QcSSCD present and/or PolicyId QCP+ (qcp-public-with-sscd) present	QSCD_YES	QSCD_YES	QSCD_NO
QcSSCD not present and PolicyId QCP+ (qcp-public-with-sscd) not present	QSCD_YES	QSCD_NO	QSCD_NO

e. The processing shall set `QSCD-Status` to the value "PROCESS_PASSED"; and
f. The processing shall stop the process.

(b) The processing shall set `QSCD-Results` to the value "QSCD_INDETERMINATE";
(c) The processing shall set `QSCD-Status` to the value "PROCESS_PASSED"; and
(d) The processing shall stop the process.

PRO-4.5.4-04: If `QC_Results` includes the value "QC_For_eSig" or "QC_For_eSeal", then considering respectively `CHECK_1_SET-OF_QE` or `CHECK_2_SET-OF_QE` as part of the outputs of the process run in PRO-4.5.4-01:

(a) The processing shall identify the set of all applicable qualifiers as per the content of the 'Qualifier' descendant elements (see clause 5.5.9.2.3 of ETSI TS 119 612 [1]) of all 'QualificationElement' elements of the considered output variable, and shall check whether the following qualifiers are present among them: 'QCWithQSCD' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD"), 'QCNoQSCD' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD"), 'QCQSCDStatusAsInCert' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDStatusAsInCert"), and 'QCQSCDManagedOnBehalf' ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf");
(b) In case one of the following combinations is found, the processing shall set `QSCD-Results` to the value "QSCD_INDETERMINATE", shall set `QSCD-Status` to the value "PROCESS_PASSED_WITH_WARNING", shall add to `QSCD-Sub-Status` the value "WARNING_Inconsistency_in_applying_qualifiers_for_QSCD_status", and shall stop the process:
   a. 'QCWithQSCD' and 'QCNoQSCD';
   b. 'QCQSCDManagedOnBehalf' and 'QCNoQSCD';
   c. 'QCQSCDStatusAsInCert' and any one of the other qualifiers listed in PRO-4.5.4-04.(a).
(c) The processing shall identify the presence of the QcSSCD statement in the QCStatements extension (see ETSI EN 319 412-5 [3]) in `CERT`;
(d) The processing shall use the information obtained in above point PRO-4.5.4-04.(a) to select the appropriate column of Table 7, shall use the information obtained in above point PRO-4.5.4-04.(c) to select the appropriate row of Table 7, and shall set `QSCD-Results` to the value found in the selected cell.

Table 7: QSCD status check (Regulation regime)

Sie:Q / CERT	"QCWithQSCD" or "QCQSCDManagedOnBehalf"	"QCQSCDStatusAsInCert" or no indication	"QCNoQSCD"
QcSSCD present	QSCD_YES	QSCD_YES	QSCD_NO
QcSSCD not present	QSCD_YES	QSCD_NO	QSCD_NO

(e) The processing shall set `QSCD-Status` to the value "PROCESS_PASSED"; and
(f) The processing shall stop the process.

PRO-4.5.4-05: If `QC_Results` does not include the value "QC_For_eSig" nor the value "QC_For_eSeal" then:

(a) The processing shall set `QSCD-Results` to the value "QSCD_INDETERMINATE";
(b) The processing shall set `QSCD-Status` to the value "PROCESS_PASSED"; and
(c) The processing shall stop the process.

4.6 EU qualified time stamp determination

4.6.1 Description

The procedure specified in clause 4.6 allows determining whether a time stamp token is confirmed by the applicable EUMS trusted list to have been an EU qualified time stamp at its generation time, provided that the timestamp is valid.

4.6.2 Inputs

Name	Description of inputs
TST	The time stamp token for which the information is to be obtained.

4.6.3 Outputs

Name	Description
QTST-Results	An indication of the EU qualified status of TST through one of the following values: (a) "Not_Qualified" to indicate that TST is not an EU qualified time stamp according to the EUMS trusted list from CC at Date-time; (b) "Qualified" to indicate that TST is an EU qualified time stamp according to the EUMS trusted list from CC at Date-time; (c) "Indeterminate" to indicate that the EUMS trusted list from CC cannot be used to confirm that TST is an EU qualified time stamp at Date-time; (d) Void.
QTST-Status	The status indication of the process.
QTST-Sub-Status	A list of indications supplementing QTST-Status indication.
CC	The country code of the EUMS trusted list being used to obtain the above listed three other outputs.

OUT-4.6.3-01: All above listed output variables shall be initialised to void.

4.6.4 Processing

PRO-4.6.4-01: The processing shall set Date-time to the date and time value as specified in TST and expressed as specified in clause 5.1.3 of ETSI TS 119 612 [1].

EXAMPLE: This date and time indication can be genTime from TSTInfo as specified in RFC 3161 [i.6].

PRO-4.6.4-02: If Date-time is before "2016-06-30T22:00:00Z", then:

(a) The processing shall set QTST-Status to the value "PROCESS_PASSED";
(b) The processing shall set QTST-Results to the value "Not_Qualified"; and
(c) The processing shall stop the process.

PRO-4.6.4-03: The processing shall set CERT to the X.509 certificate supporting the validation of the digital signature on TST.

PRO-4.6.4-04: The processing shall set CC to the country code value of the countryName attribute of the subjectName field of the certificate provided in CERT, in capital letters in accordance with the ISO 3166-1 [2] Alpha 2 country code, with, when applicable:

(a) the country code value "GB" being converted to "UK";
(b) the country code value "GR" being converted to "EL".

PRO-4.6.4-05: The processing shall set TLS-Sti to the value "http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST" as specified in clause 5.5.1.1 of ETSI TS 119 612 [1].

PRO-4.6.4-06: The processing shall run the process described in clause 4.3 of the present document, passing the following inputs to the process:

(a) `CERT`;

(b) `TLS-Sti`;

(c) `Date-time`;

(d) `CC`.

PRO-4.6.4-07: If the output `SI-Status` of the process run in PRO-4.6.4-06 has the value "PROCESS_FAILED", then:

(a) The processing shall set `QTST-Status` to the value "PROCESS_FAILED";
(b) The processing shall set `QTST-Sub-Status` to the set of values from `SI-Status` and `SI-Sub-Status`; and
(c) The processing shall stop the process.

PRO-4.6.4-08: If the output `SI-Results` of the process run in PRO-4.6.4-06 is void, then:

(a) The processing shall set `QTST-Status` to the value "PROCESS_PASSED";
(b) The processing shall set `QTST-Results` to the value "Not_Qualified"; and
(c) The processing shall stop the process.

PRO-4.6.4-09: If the output `SI-Results` of the process run in PRO-4.6.4-06 includes more than one tuple for which the `SI-at-Date-time` respective parts include different values for their respective 'Service current status' or 'Service previous status' field, then:

(a) The processing shall set `QTST-Status` to the value "PROCESS_FAILED";
(b) The processing shall set `QTST-Results` to the value "Indeterminate";
(c) The processing shall set `QTST-Sub-Status` to the value "ERROR_INCONSISTENCY_IN_TL_ON_TST_STATUS"; and
(d) The processing shall stop the process.

PRO-4.6.4-10: If the output `SI-Results` of the process run in PRO-4.6.4-06 includes more than one tuple for which the `SI-at-Date-time` respective parts include different public key values for their 'Service digital identifier' field (see clause 5.5.3 of ETSI TS 119 612 [1]), then the processing shall add to `QTST-Sub-Status` the value "WARNING_DUPLICATION_OF_SERVICE_INFORMATION_IN_TL_REGARDING_TST".

PRO-4.6.4-11: If the `organizationName` attribute of the `subjectName` field of the certificate provided in `CERT` is not matching one of the values of `TSP-Name` or `TSP-Trade-Name` of the output `SI-Results` of the process run in PRO-4.6.4-06, then:

(a) The processing shall set `QTST-Status` to the value "PROCESS_FAILED";
(b) The processing shall set `QTST-Results` to the value "Indeterminate";
(c) The processing shall set `QTST-Sub-Status` to the value "ERROR_TSP_NAME_INCONSISTENCY_BETWEEN_CERT_AND_TL"; and
(d) The processing shall stop the process.

PRO-4.6.4-12: If the 'Service current status' or 'Service previous status' field of the `SI-at-Date-time` part(s) of the output `SI-Results` of the process run in PRO-4.6.4-06 has the value "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted":

(a) Then:
    a. The processing shall set `QTST-Status` to the value "PROCESS_PASSED";
    b. The processing shall set `QTST-Results` to the value "Qualified"; and
    c. The processing shall stop the process.
(b) Else:
    a. The processing shall set `QTST-Status` to the value "PROCESS_PASSED";
    b. The processing shall set `QTST-Results` to the value "Not_Qualified"; and
    c. The processing shall stop the process.

4.7 EU qualified validation service determination

4.7.1 Description

The procedure specified in clause 4.7 allows determining whether the signer identified in the certificate supporting the validation of the digital signature of a trust service output is confirmed by the applicable EUMS trusted list to have been, at a specific date and time, an EU qualified trust service provider for the provision of a qualified validation service for qualified electronic signatures and/or for the provision of a qualified validation service for qualified electronic seals.

NOTE: The verification whether the trust service output is indeed a signature validation report attesting the result of the validation process of an EU qualified electronic signature or of an EU qualified electronic seal is out of scope of the present procedure.

4.7.2 Inputs

Name	Description of inputs
CERT	X.509 certificate for which the information is to be obtained (e.g. a ds:X509Certificate value of a ds:KeyInfo of the ds:Signature from the corresponding trust service output)
Date-time	Date and time indication as specified in clause 5.1.3 of ETSI TS 119 612 [1].

4.7.3 Outputs

Name	Description
QVSO-Results	A set of indications of the EU qualified status of the QTSP/QTS identified through the subjectName attribute of CERT, which contains one or more of the following values: (a) "Not_Qualified_For_eSig" to indicate that the signer identified in the CERT is confirmed by the applicable EUMS trusted list from CC to not have been, at Date-time, an EU qualified trust service provider for the provision of a qualified validation service for qualified electronic signatures; (b) "Not_Qualified_For_eSeal" to indicate that the signer identified in the CERT is confirmed by the applicable EUMS trusted list from CC to not have been, at Date-time, an EU qualified trust service provider for the provision of a qualified validation service for qualified electronic seals; (c) "Qualified_For_eSig" to indicate that the signer identified in the CERT is confirmed by the applicable EUMS trusted list from CC to have been, at Date-time, an EU qualified trust service provider for the provision of a qualified validation service for qualified electronic signatures; (d) "Qualified_For_eSeal" to indicate that the signer identified in the CERT is confirmed by the applicable EUMS trusted list from CC to have been, at Date-time, an EU qualified trust service provider for the provision of a qualified validation service for qualified electronic seals; (e) "Indeterminate" to indicate that the EUMS trusted list from CC cannot be used to confirm that the signer identified in the CERT has been, at Date-time, an EU qualified trust service provider for the provision of a qualified validation service for qualified electronic signatures or for the provision of a qualified validation service for qualified electronic seals; (f) Void.
QVSO-Status	The status indication of the process.
QVSO-Sub-Status	A list of indications supplementing QVSO-Status indication.

CC	The country code of the EUMS trusted list being used to obtain the above listed three other outputs.

OUT-4.7.3-01: All above listed output variables shall be initialised to void.

4.7.4 Processing

PRO-4.7.4-01: If Date-time is before "2016-06-30T22:00:00Z", then:

(a) The processing shall set QVSO-Status to the value "PROCESS_PASSED";
(b) The processing shall set QVSO-Results to the set of values "Not_Qualified_For_eSig" and "Not_Qualified_For_eSeal"; and
(c) Stop the process.

PRO-4.7.4-02: The processing shall set CC to the country code value of the countryName attribute of the subjectName field of the certificate provided in CERT, in capital letters in accordance with the ISO 3166-1 [2] Alpha 2 country code, with, when applicable:

(a) the country code value "GB" being converted to "UK";
(b) the country code value "GR" being converted to "EL".

PRO-4.7.4-03 The processing shall set TLS-Sti to the value "http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q" as specified in clause 5.5.1.1 of ETSI TS 119 612 [1].

PRO-4.7.4-04: The processing shall run the process described in clause 4.3 of the present document, passing the following inputs to the process:

(a) CERT;

(b) TLS-Sti;

(c) Date-time;

(d) CC.

PRO-4.7.4-05: If the output SI-Status of the process run in PRO-4.7.4-04 has the value "PROCESS_FAILED", then:

(a) The processing shall set QVSO-Status to the value "PROCESS_FAILED";
(b) The processing shall set QVSO-Sub-Status to the set of values from SI-Status and SI-Sub-Status; and
(c) The processing shall stop the process.

PRO-4.7.4-06: If the output SI-Results of the process run in PRO-4.7.4-04 is void, then:

(a) The processing shall set QVSO-Status to the value "PROCESS_PASSED";
(b) The processing shall set QVSO-Results to the set of values "Not_Qualified_For_eSig" and "Not_Qualified_For_eSeal"; and
(c) The processing shall stop the process.

PRO-4.7.4-07: If the output SI-Results of the process run in PRO-4.7.4-04 includes more than one tuple for which the SI-at-Date-time respective parts include different values for their 'Service current status' or 'Service previous status' field, then:

(a) The processing shall set QVSO-Status to the value "PROCESS_FAILED";
(b) The processing shall set QVSO-Results to the value "Indeterminate";
(c) The processing shall set QVSO-Sub-Status to the value "ERROR_INCONSISTENCY_IN_TL_ON_VSO-CERT_STATUS"; and
(d) The processing shall stop the process.

PRO-4.7.4-08: If the output SI-Results of the process run in PRO-4.7.4-04 includes more than one tuple for which the SI-at-Date-time respective parts include different public key values for their 'Service digital identifier' field

(see clause 5.5.3 of ETSI TS 119 612 [1]), then the processing shall add to QVSO-Sub-Status the value "WARNING_DUPLICATION_OF_SERVICE_INFORMATION_IN_TL_REGARDING_VSO-CERT".

PRO-4.7.4-09: If the organizationName attribute of the subjectName field of the certificate provided in CERT is not matching one of the values of TSP-Name or TSP-Trade-Name of the output SI-Results of the process run in PRO-4.7.4-04, then:

(a) The processing shall set QVSO-Status to the value "PROCESS_FAILED";
(b) The processing shall set QVSO-Results to the value "Indeterminate";
(c) The processing shall set QVSO-Sub-Status to the value "ERROR_TSP_NAME_INCONSISTENCY_BETWEEN_CERT_AND_TL"; and
(d) The processing shall stop the process.

PRO-4.7.4-10: If the 'Service current status' or 'Service previous status' field(s) of the SI-at-Date-time part(s) of the output SI-Results of the process run in PRO-4.7.4-04 has(have) the value "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted":

(a) Then:
  a. The processing shall set QVSO-Status to the value "PROCESS_PASSED";
  b. If one of these SI-at-Date-time respective parts include an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) including the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures":
    i. then the processing shall add to QVSO-Results the value "Qualified_For_eSig";
    ii. else the processing shall add to QVSO-Results the value "Not_Qualified_For_eSig";
  c. If one of these SI-at-Date-time respective parts include an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) including the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals":
    i. then the processing shall add to QVSO-Results the value "Qualified_For_eSeal";
    ii. else the processing shall add to QVSO-Results the value "Not_Qualified_For_eSeal"; and
  d. The processing shall stop the process.
(b) Else:
  a. The processing shall set QVSO-Status to the value "PROCESS_PASSED";
  b. The processing shall set QVSO-Results to the set of values "Not_Qualified_For_eSig" and "Not_Qualified_For_eSeal"; and
  c. The processing shall stop the process.

4.8 EU qualified preservation service determination

4.8.1 Description

The procedure specified in clause 4.8 allows determining whether the signer identified in the certificate supporting the validation of the digital signature of a trust service output is confirmed by the applicable EUMS trusted list to have been, at a specific date and time, an EU qualified trust service provider for the provision of a qualified preservation service for qualified electronic signatures and/or for the provision of a qualified preservation service for qualified electronic seals.

NOTE 1: The present process is only applicable when the qualified trust service provider providing a qualified preservation service for qualified electronic signatures and/or for qualified electronic seals is making use of PKI technology (e.g. for digitally signing evidences, attestations, reports) and the related PKI certificate is published in the applicable EUMS trusted list.

4.8.2 Inputs

Name	Description of inputs
CERT	X.509 certificate for which the information is to be obtained (e.g. a ds:X509Certificate value of a ds:KeyInfo of the ds:Signature from the corresponding trust service output)
Date-time	Date and time indication as specified in clause 5.1.3 of ETSI TS 119 612 [1].

4.8.3 Outputs

Name	Description
QPSO-Results	A set of indications of the EU qualified status of the QTSP/QTS identified through the subjectName attribute of CERT, which containsone or more of the following values: (a) "Not_Qualified_For_eSig" to indicate that the signer identified in the CERT is confirmed by the applicable EUMS trusted list from CC to not have been, at Date-time, an EU qualified trust service provider for the provision of a qualified preservation service for qualified electronic signatures; (b) "Not_Qualified_For_eSeal" to indicate that the signer identified in the CERT is confirmed by the applicable EUMS trusted list from CC to not have been, at Date-time, an EU qualified trust service provider for the provision of a qualified preservation service for qualified electronic seals; (c) "Qualified_For_eSig" to indicate that the signer identified in the CERT is confirmed by the applicable EUMS trusted list from CC to have been, at Date-time, an EU qualified trust service provider for the provision of a qualified preservation service for qualified electronic signatures; (d) "Qualified_For_eSeal" to indicate that the signer identified in the CERT is confirmed by the applicable EUMS trusted list from CC to have been, at Date-time, an EU qualified trust service provider for the provision of a qualified preservation service for qualified electronic seals; (e) "Indeterminate" to indicate that the EUMS trusted list from CC cannot be used to confirm that the signer identified in the CERT has been, at Date-time, an EU qualified trust service provider for the provision of a qualified preservation service for qualified electronic signatures or for the provision of a qualified preservation service for qualified electronic seals; (f) Void.
QPSO-Status	The status indication of the process.
QPSO-Sub-Status	A list of indications supplementing QPSO-Status indication.
CC	The country code of the EUMS trusted list being used to obtain the above listed three other outputs.

OUT-4.8.3-01: All above listed output variables shall be initialised to void.

4.8.4 Processing

PRO-4.8.4-01: If Date-time is before "2016-06-30T22:00:00Z", then:

(a) The processing shall set QPSO-Status to the value "PROCESS_PASSED";
(b) The processing shall set QPSO-Results to the set of values "Not_Qualified_For_eSig" and "Not_Qualified_For_eSeal"; and
(c) The processing shall stop the process.

PRO-4.8.4-02: The processing shall set CC to the country code value of the countryName attribute of the subjectName field of the certificate provided in CERT, in capital letters in accordance with the ISO 3166-1 [2] Alpha 2 country code with, when applicable:

(a) the country code value "GB" being converted to "UK";
(b) the country code value "GR" being converted to "EL".

PRO-4.8.4-03: The processing shall set TLS-Sti to the value "http://uri.etsi.org/TrstSvc/Svctype/PSES/Q" as specified in clause 5.5.1.1 of ETSI TS 119 612 [1].

PRO-4.8.4-04: The processing shall run the process described in clause 4.3 of the present document, passing the following inputs to the process:

(a) `CERT`;

(b) `TLS-Sti`;

(c) `Date-time`;

(d) `CC`.

PRO-4.8.4-05: If the output `SI-Status` of the process run in PRO-4.8.4-04 has the value "PROCESS_FAILED", then:

(a) The processing shall set `QPSO-Status` to the value "PROCESS_FAILED";
(b) The processing shall set `QPSO-Sub-Status` to the set of values from `SI-Status` and `SI-Sub-Status`; and
(c) The processing shall stop the process.

PRO-4.8.4-06: If the output `SI-Results` of the process run in PRO-4.8.4-04 is void, then:

(a) The processing shall set `QPSO-Status` to the value "PROCESS_PASSED";
(b) The processing shall set `QPSO-Results` to the set of values "Not_Qualified_For_eSig" and "Not_Qualified_For_eSeal"; and
(c) The processing shall stop the process.

PRO-4.8.4-07: If the output `SI-Results` of the process run in PRO-4.8.4-04 includes more than one tuple for which the `SI-at-Date-time` respective parts include different values for their 'Service current status' or 'Service previous status' field, then:

(a) The processing shall set `QPSO-Status` to the value "PROCESS_FAILED";
(b) The processing shall set `QPSO-Results` to the value "Indeterminate";
(c) The processing shall set `QPSO-Sub-Status` to the value "ERROR_INCONSISTENCY_IN_TL_ON_PSO-CERT_STATUS"; and
(d) The processing shall stop the process.

PRO-4.8.4-08: If the output `SI-Results` of the process run in PRO-4.8.4-04 includes more than one tuple for which the `SI-at-Date-time` respective parts include different public key values for their 'Service digital identifier' field (see clause 5.5.3 of ETSI TS 119 612 [1]), then the processing shall add to `QPSO-Sub-Status` the value "WARNING_DUPLICATION_OF_SERVICE_INFORMATION_IN_TL_REGARDING_PSO-CERT".

PRO-4.8.4-09: If the `organizationName` attribute of the `subjectName` field of the certificate provided in `CERT` is not matching one of the values of `TSP-Name` or `TSP-Trade-Name` of the output `SI-Results` of the process run in PRO-4.7.4-04, then:

(a) The processing shall set `QPSO-Status` to the value "PROCESS_FAILED";
(b) The processing shall set `QPSO-Results` to the value "Indeterminate";
(c) The processing shall set `QPSO-Sub-Status` to the value "ERROR_TSP_NAME_INCONSISTENCY_BETWEEN_CERT_AND_TL"; and
(d) The processing shall stop the process.

PRO-4.8.4-10: If the 'Service current status' or 'Service previous status' field(s) of the `SI-at-Date-time` part(s) of the output `SI-Results` of the process run in PRO-4.8.4-04 has the value "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted":

(a) Then:
    a. The processing shall set `QPSO-Status` to the value "PROCESS_PASSED";
    b. If one of these `SI-at-Date-time` respective parts include an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) including the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures":
        i. then the processing shall add to `QPSO-Results` the value "Qualified_For_eSig";
        ii. else the processing shall add to `QPSO-Results` the value "Not_Qualified_For_eSig";

c. If one of these SI-at-Date-time respective parts include an 'additionalServiceInformation' extension (see clause 5.5.9.4 of ETSI TS 119 612 [1]) including the value "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals":
   i. then the processing shall add to QPSO-Results the value "Qualified_For_eSeal";
   ii. else the processing shall add to QPSO-Results the value "Not_Qualified_For_eSeal"; and
d. The processing shall stop the process.

(b) Else:
a. The processing shall set QPSO-Status to the value "PROCESS_PASSED";
b. The processing shall set QPSO-Results to the set of values "Not_Qualified_For_eSig" and "Not_Qualified_For_eSeal"; and
c. The processing shall stop the process.

4.9 EU qualified electronic registered delivery service determination

4.9.1 Description

The procedure specified in clause 4.9 allows determining whether the signer identified in the certificate supporting the validation of the digital signature of a trust service output is confirmed by the applicable EUMS trusted list to have been, at a specific date and time, an EU qualified trust service provider for the provision of a qualified electronic registered delivery service.

NOTE: The verification whether the trust service output is indeed a qualified electronic registered delivery service evidence or statement is out of scope of the present procedure.

4.9.2 Inputs and parameters

Name	Description of inputs
CERT	X.509 certificate for which the information is to be obtained (e.g. a ds:X509Certificate value of a ds:KeyInfo of the ds:Signature from the corresponding trust service output)
Date-time	A date and time indication as specified in clause 5.1.3 of ETSI TS 119 612 [1].

4.9.3 Outputs

Name	Description
QERDSO-Results	An indication of the EU qualified status of the QTSP/QTS identified through the subjectName attribute of CERT, which is one of the following values: (a) "Not_Qualified" to indicate that the signer identified in the CERT is confirmed by the applicable EUMS trusted list from CC to not have been, at Date-time, an EU qualified trust service provider for the provision of a qualified electronic registered delivery service; (b) "Qualified" to indicate that the signer identified in the CERT is confirmed by the applicable EUMS trusted list from CC to have been, at Date-time, an EU qualified trust service provider for the provision of a qualified electronic registered delivery service; (c) "Indeterminate" to indicate that the EUMS trusted list from CC cannot be used to confirm that the signer identified in the CERT has been, at Date-time, an EU qualified trust service provider for the provision of a qualified electronic registered delivery service; (d) Void.
QERDSO-Status	The status indication of the process.

QERDSO-Sub-Status	A list of indications supplementing QERDSO-Status indication.
CC	The country code of the EUMS trusted list being used to obtain the above listed three other outputs.

OUT-4.9.3-01: All above listed output variables shall be initialised to void.

4.9.4 Processing

PRO-4.9.4-01: If Date-time is before "2016-06-30T22:00:00Z", then:

(a) The processing shall set QERDSO-Status to the value "PROCESS_PASSED";
(b) The processing shall set QERDSO-Results to the value "Not_Qualified"; and
(c) The processing shall stop the process.

PRO-4.9.4-02: The processing shall set CC to the country code value of the countryName attribute of the subjectName field of the certificate provided in CERT, in capital letters in accordance with the ISO 3166-1 [2] Alpha 2 country code, with, when applicable:

(a) The country code value "GB" being converted to "UK";
(b) The country code value "GR" being converted to "EL".

PRO-4.9.4-03: The processing shall set TLS-Sti-1 to the value "http://uri.etsi.org/TrstSvc/Svctype/EDS/Q" as specified in clause 5.5.1.1 of ETSI TS 119 612 [1].

PRO-4.9.4-04: The processing shall set TLS-Sti-2 to the value "http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q" as specified in clause 5.5.1.1 of ETSI TS 119 612 [1].

PRO-4.9.4-05: The processing shall run the process described in clause 4.3 of the present document, passing the following inputs to the process:

(a) CERT;

(b) TLS-Sti-1;

(c) Date-time;

(d) CC.

PRO-4.9.4-06: The processing shall run the process described in clause 4.3 of the present document, passing the following inputs to the process:

(a) CERT;

(b) TLS-Sti-2;

(c) Date-time;

(d) CC.

PRO-4.9.4-07: If both outputs SI-Status of the processes run in PRO-4.9.4-05 and in PRO-4.9.4-06 have the value "PROCESS_FAILED", then:

(a) The processing shall set QERDSO-Status to the value "PROCESS_FAILED";
(b) The processing shall set QERDSO-Sub-Status to the set of values from SI-Status and SI-Sub-Status of both processes; and
(c) The processing shall stop the process.

PRO-4.9.4-08: If both outputs SI-Results of the processes run in PRO-4.9.4-05 and in PRO-4.9.4-06 are void, then:

(a) The processing shall set QERDSO-Status to the value "PROCESS_PASSED";
(b) The processing shall set QERDSO-Results to the value "Not_Qualified"; and
(c) The processing shall stop the process.

PRO-4.9.4-09: If one of the outputs SI-Results of the processes run in PRO-4.9.4-05 and in PRO-4.9.4-06 includes more than one tuple for which the SI-at-Date-time respective parts include different values for their 'Service current status' or 'Service previous status' field, then:

(a) The processing shall set QERDSO-Status to the value "PROCESS_FAILED";
(b) The processing shall set QERDSO-Results to the value "Indeterminate";
(c) The processing shall set QERDSO-Sub-Status to the value "ERROR_INCONSISTENCY_IN_TL_ON_ERDS_CERT_STATUS"; and
(d) The processing shall stop the process.

PRO-4.9.4-10: If one of the outputs SI-Results of the processes run in PRO-4.9.4-05 and in PRO-4.9.4-06 includes more than one tuple for which the SI-at-Date-time respective parts include different public key values for their 'Service digital identifier' field (see clause 5.5.3 of ETSI TS 119 612 [1]), then the processing shall add to QERDSO-Sub-Status the value "WARNING_DUPLICATION_OF_SERVICE_INFORMATION_IN_TL_REGARDING_ERDS_CERT".

PRO-4.9.4-11: When the SI-Results tuples from the processes run in PRO-4.9.4-05 and in PRO-4.9.4-06 include different TSP-Name values, then:

(a) The processing shall add to QERDSO-Sub-Status the indication value "ERROR_TSP_CONFLICT";
(b) The processing shall set QERDSO-Status to the value "PROCESS_FAILED"; and
(c) The processing shall stop the process.

PRO-4.9.4-12: If the organizationName attribute of the subjectName field of the certificate provided in CERT is not matching one of the values of TSP-Name or TSP-Trade-Name of all not void tuples from all tuples from output SI-Results of the processes run in PRO-4.9.4-05 and in PRO-4.9.4-06, then:

(a) The processing shall set QERDSO-Status to the value "PROCESS_FAILED";
(b) The processing shall set QERDSO-Results to the value "Indeterminate";
(c) The processing shall set QERDSO-Sub-Status to the value "ERROR_TSP_NAME_INCONSISTENCY_BETWEEN_ERDS_CERT_AND_TL"; and
(d) The processing shall stop the process.

PRO-4.9.4-13: If the 'Service current status' or 'Service previous status' field(s) of the SI-at-Date-time part(s) of the output(s) SI-Results of any of the processes run in PRO-4.9.4-05 and in PRO-4.9.4-06 has(have) the value "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted":

(a) Then:
    a. The processing shall set QERDSO-Status to the value "PROCESS_PASSED";
    b. The processing shall set QERDSO-Results to the value "Qualified"; and
    c. The processing shall stop the process.
(b) Else:
    a. The processing shall set QERDSO-Status to the value "PROCESS_PASSED";
    b. The processing shall set QERDSO-Results to the value "Not_Qualified"; and
    c. The processing shall stop the process.

History

Document history		
V0.0.1	08.02.2018	Creation of the document.
V0.0.2	12.02.2018	Update of the document.
V0.0.3	21.03.2018	Update of the document.
V0.0.4	18.06.2018	Update of the document.
V0.0.5	28.06.2018	Update of the document.
V0.0.6	24.09.2018	Update of the document – stable draft.
V0.0.7	20.03.2019	Final draft.
V0.0.8	07.06.2019	Updated draft from ESI#67.
V0.0.9	31.07.2019	Updated draft from comments on v0.0.8.