



Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing qualified trust service providers against the eIDAS Regulation requirements

FINAL DRAFT BEFORE APPROVAL

Send comments **ONLY** to E-SIGNATURES_COMMENTS@list.etsi.org

by 30 October 2018

Download the template for comments:

[https://docbox.etsi.org/ESI/Open/Latest Drafts/Template-for-comments.doc](https://docbox.etsi.org/ESI/Open/Latest%20Drafts/Template-for-comments.doc)

CAUTION: This **DRAFT document** is provided for information and is for future development work within the ETSI Technical Committee ESI only. ETSI and its Members accept no liability for any further use/implementation of this Specification.

Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation

Service at

<http://www.etsi.org/standards-search>

Reference

DTS/ESI-0019403-3

Keywords

conformity, e-commerce, electronic signature,
security, trust services

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
oneM2M logo is protected for the benefit of its Members.
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references	5
3 Definitions and abbreviations.....	7
3.1 Definitions	7
3.2 Abbreviations.....	7
3.3 Notation	8
4 Requirements for CABs assessing QTSP/QTSs against requirements of Regulation (EU) No 910/2014.....	8
4.1 Conformity assessment scheme	8
4.2 Conformity assessment report.....	9
Annex A (informative): QTSP/QTS conformity assessment against Regulation (EU) No 910/2014	14
A.1 Overview	14
Annex B (informative): Bibliography	16
History	17

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

ISO/IEC 17065 [i.30] is an international standard which specifies general requirements for conformity assessment bodies (CABs) performing certification of products, processes, or services. These requirements are not focussed on any specific application domain where CABs work.

In ETSI EN 319 403 [1] the general requirements of [i.30] are supplemented to provide additional dedicated requirements for CABs performing certification of trust service providers (TSPs) and the trust services they provide towards defined criteria against which they claim conformance.

ETSI EN 319 403 [1] aims to meet the general needs of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.1], and from CA/Browser Forum [i.4]. It aims include support of national accreditation bodies (NABs) as specified in Regulation (EC) No. 765/2008 [i.3] in applying ISO/IEC 17065 [i.30] for the accreditation of CABs that certify TSPs and the trust services they provide so that this is carried out in a consistent manner. In accordance with [i.3], attestations issued by conformity assessment bodies accredited by a NAB can be formally recognized across Europe. ETSI EN 319 403 [1] supplements ISO/IEC 17065 [i.30] by specifying additional requirements, e.g. on resources, on the assessment process and on the audit of a TSP's management system, as defined in ISO/IEC 17021 [i.6] and in ISO/IEC 27006 [i.7].

The present document specifies supplementary requirements to those defined in [1] in order to provide additional dedicated requirements for CABs performing certification of qualified trust service providers (QTSPs) and the qualified trust services (QTSs) they provide towards the requirements of Regulation (EU) No 910/2014 [i.1]. It aims supporting NABs for the accreditation of CABs in line with Article 3.18 of Regulation (EU) No 910/2014 [i.1].

The ENISA technical guidelines on trust services "Guidelines on initiation of qualified trust services" [i.9] have been used as basis for the present document.

1 Scope

The present document defines specific supplementary requirements for the application of ETSI EN 319 403 [1] to conformity assessments (audits) of qualified trust service providers (QTSPs) and the qualified trust services (QTSs) they provide, as well as of trust service providers, without qualified status, intending to start providing qualified trust services, against the requirements of Regulation (EU) No 910/2014 [i.1] assuming the use of ETSI policy requirement standards but not precluding use of other specifications.

In particular, the present document defines requirements for conformity assessment reports, including their content.

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 EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".
- [2] ETSI TS 119 612 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".
- [3] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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.

NOTE: 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.

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

- [i.3] EC Regulation No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.
- [i.4] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.
- [i.5] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardisation of signatures; Definitions and abbreviations".
- [i.6] ISO/IEC 17021-1: "Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements".
- [i.7] ISO/IEC 27006: "Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems".
- [i.8] Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services.
- NOTE: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2015.128.01.0013.01.ENG
- [i.9] ENISA: "Guidelines on initiation of qualified trust services; Technical guidelines on trust services", December 2017. ISBN: 978-92-9204-189-2.
- NOTE: <https://www.enisa.europa.eu/publications/tsp-initiation>
- [i.10] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- [i.11] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
- [i.12] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
- [i.13] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".
- [i.14] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".
- [i.15] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".
- [i.16] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".
- [i.17] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
- [i.18] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
- [i.19] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".
- [i.20] ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services".
- [i.21] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".
- [i.22] ETSI TS 119 102-2: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report".

- [i.23] ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists".
- [i.24] ETSI TS 119 511: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques".
- [i.25] ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services".
- [i.26] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy & security requirements for electronic registered delivery service providers".
- [i.27] ETSI EN 319 522: "Electronic Signatures and Infrastructures (ESI); Electronic registered delivery services".
- [i.28] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy & security requirements for registered electronic mail (REM) service providers".
- [i.29] ETSI EN 319 532: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services".
- [i.30] ISO/IEC 17065: "Conformity assessment -- Requirements for bodies certifying products, processes and services".
- [i.31] CEN EN 419 221-5: "Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services".
- [i.32] CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: Security Requirements for Trustworthy Systems Supporting Server Signing".
- [i.33] CEN EN 419 241-2: "Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing".
- [i.34] ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".
- [i.35] ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".
- [i.36] ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 119 001 [i.5] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 119 001 [i.5] apply, as well as the following abbreviations:

CAB	Conformity Assessment Body
CAR	Conformity Assessment Report

CID	Commission Implementing Decision
HSM	Hardware Security Module
NAB	National Accreditation Body
PEM	Privacy-Enhanced Electronic Mail
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
SB	Supervisory Body

3.3 Notation

The requirements in the present document are identified as follows:

<3 letters identifying the section title> - <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 Requirements for CABs assessing QTSP/QTSs against requirements of Regulation (EU) No 910/2014

4.1 Conformity assessment scheme

CAS-4.1-01: The conformity assessment scheme for which a CAB is accredited to assess QTSP/QTSs against the requirements of Regulation (EU) No 910/2014 [i.1] in accordance with Regulation (EC) No 765/2008 [i.3] shall be defined in a way that such accreditation ensures the accredited CAB is competent to carry out conformity assessment of a QTSP/QTS against the requirements of Regulation (EU) No 910/2014 [i.1].

In particular:

CAS-4.1-02: The conformity assessment scheme shall, with the aim of confirming that the assessed QTSP/QTS fulfils the applicable requirements from Regulation (EU) No 910/2014 [i.1], include:

- Requirements on the CAB, including on the auditing rules under which the CAB will carry out its conformity assessment and on the effective set of criteria, meeting at least requirements from ETSI EN 319 403 [1], and

NOTE: This de facto implies the CAB being compliant with ETSI EN 319 403[1], hence with ISO/IEC 17065 [i.30], to be a certification body and the conformity assessment scheme to be a certification scheme [i.30].

- Control objectives and controls against which the CAB will assess a QTSP/QTS against the applicable requirements of Regulation (EU) No 910/2014 [i.1];

CAS-4.1-03: The resulting conformity assessment report shall meet the requirements of clause 4.2 of the present document.

4.2 Conformity assessment report

CAR-4.2-01: The conformity assessment report (CAR) shall bear a clear certification decision conformant to clause 7.6 of ETSI EN 319 403 [1], confirming - if such is the case - that the assessed QTSP/QTS meet all the applicable requirements of Regulation (EU) No 910/2014 [i.1].

CAR-4.2-02: The CAR shall provide sufficient details to demonstrate that the assessed QTSP/QTS fulfil the requirements laid down in Regulation (EU) No 910/2014 [i.1].

NOTE 1: Those details and information demonstrating QTSP/QTS compliance with Regulation (EU) No 910/2014 [i.1] requirements can be included by reference to other reports, e.g. such as audit reports against technical standards, which contain detailed and herewith sufficient information for the SB to judge the QTSP/QTS conformity to the Regulation. On top of that the SB can be pointed to the security documentation of the QTSP, like the security concept, its declaration of practices and/or of policies, etc., as it can be referenced in the CAR.

In particular:

CAR-4.2-03: The CAR shall identify the name of the CAB, and where applicable its registration number, as stated in the official records, its official postal address and its electronic address;

CAR-4.2-04: The CAR shall identify:

- (a) the name of the NAB having accredited the CAB,
- (b) the link, on the official website of the NAB, to the accreditation certificate issued by the NAB to the CAB, and
- (c) when not mentioned in the accreditation certificate:
 - (i) the scheme under which the CAB has been accredited in the context of Regulation (EU) No.765/2008 [i.3]; and

EXAMPLE 1: Such a scheme can be ISO/IEC 17065 [i.30] being completed by ETSI EN 319 403 [1].

- (ii) the conformity assessment (certification) scheme for which the CAB has been accredited to conduct conformity assessment of QTSP/QTSs against the requirements laid down in Regulation (EU) No 910/2014 [i.1];

CAR-4.2-05: The complete CAR shall be considered as part of the certification documentation specified in clause 7.7 of ETSI EN 319 403 [1];

CAR-4.2-06: The CAR shall include the accredited conformity assessment (certification) scheme document or a link to the location from where that document is available;

CAR-4.2-07: The CAR shall bear EU qualified electronic signature(s) identifying the name and title of the CAB responsible person(s) having authorised the certification decision;

CAR-4.2-08: The CAR shall be dedicated to one and only one QTSP, in particular:

- (a) the CAR shall identify the name of the assessed QTSP, and where applicable its registration number, as stated in the official records, its official postal address and its electronic address, and
- (b) when applicable, the CAR shall identify this same information of all subsidiaries, affiliated legal entities and (sub)contractors that are operating trust service components in scope of the provision of (Q)TS by the QTSP, and hence in scope of the certification decision;

NOTE 2: QTSPs can make use of third parties, whether (Q)TSPs or not, to operate part or all of the service components of the QTS they provide. In this situation, the QTSP remains the final entity responsible and liable for the QTS it provides and needs to document and ensure correct implementation of those service components against its declared practices and policies as well as against Regulation (EU) No 910/2014 [i.1].

CAR-4.2-09: The CAR shall identify, in accordance with clause 5.5.3 of ETSI TS 119 612 v2.1.1 [2], the service digital identity(ies) per type of QTS for which the CAR confirms the conformity with the requirements of Regulation (EU) No 910/2014 [i.1] providing at least:

- (a) the Subject Key Identifier as defined in RFC 5280 [3];
- (b) the Base64 PEM representation of the associated X.509v3 digital certificate;
- (c) when applicable, an indication whether specific sets or subsets of end-entity certificates issued by or under the service digital identity are excluded from the certification decision and on the basis of which criteria they can be identified;

EXAMPLE 2: Such criteria can be a list of certificate policy identifiers to match with the content of the CertificatePolicy certificate extension as defined in RFC 5280 [3] or other criteria as defined in clause 5.5.9.2.2 of ETSI TS 119 612 v2.1.1 [2].

- (d) an indication whether the service digital identity relates to an end-entity or a certification authority, clarifying whether an issuing, intermediate or root; and
- (e) an indication on how the service digital identity is used in the context of the corresponding QTS;

EXAMPLE 3: The private key corresponding to the service digital identity can be used to digitally sign (qualified) certificates, qualified electronic time stamps, evidences in the context of qualified electronic registered delivery, in the context of qualified validation of qualified electronic signatures or seals, or in the context of qualified preservation of qualified electronic signatures or seals.

CAR-4.2-10: In line with CAR-4.2-09, per type of QTS and for all service digital identities identified in CAR-4.2-09, the CAR shall provide a detailed description of the PKI functional hierarchy with the purpose to allow identification of the service entry(ies) to be listed in the applicable national trusted list in accordance with CID (EU) 2015/1505 [i.2], including at least:

- (a) the illustration of the PKI hierarchy identifying the root certification authority(ies), the intermediate certification authority(ies), the issuing certification authority(ies) and the certification paths between them;
- (b) the identification of each certification authority illustrated in point (a) through the Subject Key Identifier as defined in RFC 5280 [3];
- (c) for each of the issuing CAs identified in point (b), the list of the different (policy) sets of certificates such a CA is issuing, with for each set:
 - (i) a criteria that unambiguously identifies the certificates of the set, being either a list of certificate policy identifiers to match with the content of the CertificatePolicy certificate extension as defined in RFC 5280 [3] or other criteria as defined in clause 5.5.9.2.2 of ETSI TS 119 612 v2.1.1 [2];
 - (ii) an indication whether the certificates of the set are either qualified or non-qualified;
 - (iii) an indication whether the certificates of the set are either for electronic signatures, or for electronic seals, or for web site authentication or for none of these purposes and, in particular in this latter case, for which other purposes they are aimed to be used;

CAR-4.2-11: Pursuant the conclusions of the conformity assessment, the CAR shall provide an indication of the corresponding content of the applicable national trusted list [i.1], [i.2], which reflects the result of the assessment;

CAR-4.2-12: In line with CAR-4.2-10, the CAR shall include an exhaustive list of third parties (e.g. subcontractors) which provide/operate QTS components or service components by indicating their name, as identified in CAR-4.2-08.(b), together with the location of the sites where the corresponding component services are operated;

CAR-4.2-13: The CAR shall detail, in line with CAR-4.2-12, which of these third parties and which sites have been subject to the audit and to which extent;

CAR-4.2-14: The CAR shall identify the exhaustive list of public and QTSP internal documents, including versioning, which have been part of the scope of the audit, including at least:

- (a) The following public documents:
 - (i) The declaration of the practices used by the QTSP to provide the assessed QTS;

- (ii) The QTS policy(ies), i.e. the set of rules that indicates the applicability of the QTS to a particular community and/or class of application with common security requirements;
 - (iii) The terms and conditions related to subscriber agreements;
- (b) The following internal documents:
- (i) The termination plan referred to in Art.24.2.(i) of Regulation (EU) No 910/2014 [i.1];
 - (ii) The documentation related to the assessment of risks aimed at supporting the demonstration of the requirements of Art.19.1 of [i.1];
 - (iii) A security and personal data breach notification plan aimed to support demonstration of the requirement of Art.19.2 of [i.1]; and
 - (iv) The list of all internal documents supporting the declaration of the practices used by the QTSP to provide the assessed QTS under the corresponding QTS policy(ies); and
- (c) The following public or internal documents:
- (i) Memorandum and Articles of Association of the assessed QTSP;
 - (ii) Evidence that the assessed QTSP, in accordance with national law, maintains sufficient financial resources and/or has obtained appropriate liability insurance with regards to the provision of the QTS;

EXAMPLE 4: Evidences can include a copy of the profit and loss account and balance sheets for the last three years for which accounts have been closed, appropriate statements from banks and/or liability insurance statements.

- (iii) The list of standards on the one side with which operations are claimed to be compliant and on the other side with which operations are audited, evaluated, certified or assessed to be compliant together with details about the underlying audit, evaluation, certification or assessment scheme;
- (iv) The list of QSCDs and their certification related information when the (Q)TSP delivers such devices to its users; and
- (v) The list of devices used by the (Q)TSP as trustworthy devices (e.g. HSMs) to protect its own keys, and their certification related information, when the (Q)TSP uses such devices to secure the processes supporting the QTS it provides or aim to provide;

CAR-4.2-15: The CAR shall identify, for each stage of the audit (e.g. documentation audit and implementation audit including onsite inspections), the period during which the audit has been conducted (elapsed time) and the effort in man-days engaged by the CAB to conduct the audit;

CAR-4.2-16: The CAR shall provide, for each of the following requirements of Regulation (EU) No 910/2014 [i.1], an assessment report, with an indication of the non-conformities and their level of criticality, on the fulfilment by the assessed QTSP/QTS of the identified requirement, and/or when appropriate, on the existence of proper procedures and management system for handling this requirement:

- (a) General requirements for QTSPs and for each type of QTS provided with an indication of the relevant articles of the eIDAS Regulation:
 - (i) Article 5 regarding data processing and protection:
 - 1. As the assessment of that requirement can be seen as a duplication of point (j) of Art.24.2 of Regulation (EU) No 910/2014, reference may be made to the report on the assessment of compliance with point (j) of Art.24.2 (see below);
 - (ii) Articles 13.2 and 13.3 regarding liability and burden of the proof;
 - (iii) Article 15 regarding accessibility for person with disabilities;
 - (iv) Article 19.1 regarding risk based security due diligence;
 - (v) Article 19.2 regarding security and personal data breach notification;

- (vi) Article 20.1 regarding completion and internal procedures for completing at least 2-yearly audits and timely submission of the results to the competent SB;
 - (vii) Article 23 on the correct use of the EU trust mark for qualified trust services, including provisions from CIR (EU) 2015/806 [i.8];
 - (viii) Points (a) to (j) of Article 24.2;
- (b) Additional specific requirements for the applicable type of QTS:
- (i) Provision of qualified certificates for electronic signatures:
 - 1. Points (a) to (d) of Article 24.1;
 - 2. Article 24.2.(k);
 - 3. Article 24.3;
 - 4. Article 24.4;
 - 5. Article 28.1 (including Annex I);
 - 6. Article 28.2;
 - 7. Article 28.3;
 - 8. Article 28.4;
 - 9. Article 28.5;
 - (ii) Provision of qualified certificates for electronic seals:
 - 1. Points (a) to (d) of Article 24.1;
 - 2. Article 24.2.(k);
 - 3. Article 24.3;
 - 4. Article 24.4;
 - 5. Article 38.1 (including Annex III);
 - 6. Article 38.2;
 - 7. Article 38.3;
 - 8. Article 38.4;
 - 9. Article 38.5;
 - (iii) Provision of qualified certificates for website authentication:
 - 1. Points (a) to (d) of Article 24.1;
 - 2. Article 24.2.(k);
 - 3. Article 24.3;
 - 4. Article 24.4;
 - 5. Article 45.1 (including Annex IV);
 - (iv) Qualified validation service for qualified electronic signatures: Article 32.1, Article 32.2, Article 33.1;
 - (v) Qualified validation service for qualified electronic seals: Article 40;
 - (vi) Qualified preservation service for qualified electronic signatures: Article 34.1;
 - (vii) Qualified preservation service for qualified electronic seals: Article 40;

(viii) Qualified electronic time stamps: Article 42.1;

(ix) Qualified electronic registered delivery services: Article 44.1;

CAR-4.2-17: The CAR shall, referring to CAR-4.2-16, identify in the corresponding specific requirement report the detailed audit controls and control objectives that have been conducted during the audit with an indication of each non-conformity and their level of criticality or include a reference to separately available audit reports in which such information is included, provided such separated reports are issued by CABs, when applicable, accredited under Article 3.18 of Regulation (EU) No 910/2014 [i.1] and are endorsed by the CAB issuing the CAR;

NOTE 3: Including reference to separately available audit reports allows CARs to be built upon separated "module-conformity-reports" with regard to well-defined parts of trust services that can be reused by CABs provided such separated reports are issued by CABs accredited under Art.3(18) of Regulation (EU) No 910/2014 [i.1] and are endorsed by the CAB issuing the CAR.

CAR-4.2-18: The CAR shall include the scope, the description and the results of a significant set of test or production samples and their assessment for all relevant and applicable types of outputs from the assessed QTS;

EXAMPLE 5: Providing a single signed or sealed validation report for the validation of a single qualified electronic signature or seal is not likely to be considered as a significant set of test or production samples. The provision and assessment of a test plan including a significant set of positive and negative test cases for signatures/seals together with generated validation reports and their assessment can be an example of a significant set of samples.

CAR-4.2-19: In addition to the certification statement referred to in CAR-4.2-01, the CAR shall include, when applicable and when the conformity of the assessed QTSP/QTS is additionally certified as compliant against a specific standard or publicly available specifications, the report on the fulfilment by the QTSP and by the implementation of its QTS against such standard or specifications that has been conducted during the audit, with an indication of the non-conformities and their level of criticality;

NOTE 4: With regards to CAR-4.2-16, CAR-4.2-17, and CAR-4.2-19, pending non-conformities are only acceptable in line with clause 7.6 b) of ETSI EN 319 403 [1].

CAR-4.2-20: The CAR shall indicate:

- (a) by when, when applicable, the next surveillance audit has to be conducted at the latest, and
- (b) by when the next compliance audit has to be conducted at the latest;

CAR-4.2-21: The CAR shall indicate, in line with clause 7.6 b) of ETSI EN 319 403 [1], under which circumstances a CAB accredited under Article 3.18 of Regulation (EU) No 910/2014 [i.1] has to be involved in reassessing the assessed QTSP/QTS in addition to the planned audits; and

CAR-4.2-22: The CAR shall contain an explicit declaration stating that the certification documents, including the CAR, are also intended for the use by SBs as defined in Regulation (EU) No 910/2014 [i.1].

Annex A (informative): QTSP/QTS conformity assessment against Regulation (EU) No 910/2014

A.1 Overview

Conformity assessment bodies (CABs) aiming to assess qualified trust service providers and the qualified trust services they provide (QTSP/QTSs) against the requirements of Regulation (EU) No 910/2014 [i.1] are required by Article 3.18 of this Regulation to be accredited in accordance with Regulation (EC) No 765/2008 [i.3] in a way that such accreditation ensures the accredited CABs are competent to carry out conformity assessment of a QTSP/QTS against the requirements of the eIDAS Regulation [i.1].

The sole certificate of conformity of a QTSP/QTS against any standard is not sufficient to confirm that QTSP/QTS fulfils the requirements laid down in Regulation (EU) No 910/2014 [i.1] as required by Article 20.1 and Article 21.1 of this Regulation. No secondary legislation has been adopted yet to refer to any standard whose compliance would lead to the presumption of compliance with a sub-set of those requirements. Regulation (EU) No 910/2014 does not even foresee such secondary legislation for all the requirements applicable to QTSP/QTSs.

It is however assumed that the demonstration of QTSP/QTS compliance with specific international or European standards will facilitate demonstrating and certifying QTSP/QTS compliance with the applicable requirements of Regulation (EU) No 910/2014 [i.1]. In particular, CEN, CENELEC and ETSI have published a wide set of standards with that objective. The following table A.1 provides the list of relevant standards whose compliance is aimed to facilitate demonstration of compliance with requirements from [i.1]:

Table A.1: Standards available in support of Regulation (EU) No 910/2014 [i.1]

Qualified trust service in Regulation (EU) No 910/2014 [i.1]	Standards
Provision of qualified certificates for electronic signatures	ETSI EN 319 411-2 [i.12] (requiring compliance with ETSI EN 319 401 [i.10], EN 319 411-1 [i.11], EN 319 412-2 [i.13], EN 319 412-5 [i.16])
Provision of qualified certificates for electronic seals	ETSI EN 319 411-2 [i.12] (requiring compliance with ETSI EN 319 401 [i.10], EN 319 411-1 [i.11], EN 319 412-3 [i.14], EN 319 412-5 [i.16])
Provision of qualified certificates for website authentication	ETSI EN 319 411-2 [i.12] (requiring compliance with ETSI EN 319 401 [i.10], EN 319 411-1 [i.11], EN 319 412-4 [i.15], EN 319 412-5 [i.16])
Provision of qualified time stamps	ETSI EN 319 421 [i.17] (requiring compliance with ETSI EN 319 401 [i.10]) ETSI EN 319 422 [i.18]
Qualified validation service for qualified electronic signatures	ETSI TS 119 441 [i.19] (requiring compliance with ETSI EN 319 401 [i.10]) ETSI TS 119 442 [i.20] ETSI EN 319 102-1 [i.21], ETSI TS 119 102-2 [i.22] ETSI TS 119 172-4 [i.23]
Qualified validation service for qualified electronic seals	ETSI TS 119 441 [i.19] (requiring compliance with ETSI EN 319 401 [i.10]) ETSI TS 119 442 [i.20] ETSI EN 319 102-1 [i.21], ETSI EN 319 102-2 [i.22] ETSI TS 119 172-4 [i.23]
Qualified preservation service for qualified electronic signatures	ETSI EN 319 401 [i.10] ETSI TS 119 511 [i.24], ETSI TS 119 512 [i.25]
Qualified preservation service for qualified electronic seals	ETSI EN 319 401 [i.10] ETSI TS 119 511 [i.24], ETSI TS 119 512 [i.25]
Qualified electronic registered delivery services	ETSI EN 319 401 [i.10] ETSI EN 319 521 [i.26], ETSI EN 319 522 [i.27] ETSI EN 319 531 [i.28], ETSI EN 319 532 [i.29]

In order to meet Article 3.18 of Regulation (EU) No 910/2014 [i.1], CABs need to be accredited to carry out conformity assessment of a QTSP/QTS against the requirements of [i.1] on the basis of a conformity assessment scheme that includes requirements on CABs, requirements on the auditing rules under which CABs will carry out their conformity assessment and the effective set of criteria, control objectives and controls against which it will assess a QTSP/QTS with the aim of confirming that it fulfils the eIDAS Regulation [i.1] requirements. Such eIDAS compliant conformity assessment scheme can be defined by the CAB itself, by a competent EU MS supervisory body, or by any other body possessing the necessary technical competence.

CABs need to make sure that the resulting conformity assessment report to be submitted by the assessed QTSP to the supervisory body, whether in the context of a 2-yearly regular audit (Art.20.1 of [i.1]) and potential associated surveillance audit(s) (cfr clause 4.5 of [1]), an ad hoc audit (Art.20.2 of [i.1]) or an initiation audit (Art.21.1 of [i.1]) is such that it confirms - if such is the case - that the assessed (Q)TSP/(Q)TS fulfil all the applicable QTSP/QTS requirements of the eIDAS Regulation [i.1].

Since it is ultimately the competent supervisory body to which the CAR is notified by the assessed QTSP that will take the decision to grant or not the qualified status to the assessed QTSP/QTS, the notified CAR needs to contain sufficient information to demonstrate, in detail to the SB, that the assessed QTSP/QTS fulfils the requirements laid down in the eIDAS Regulation [i.1] and consequently deserves to be granted the qualified status.

In the context of a QTSP generating or managing electronic signature creation data on behalf of the signatory as part of the requirements of Annex II of Regulation (EU) No 910/2014 [i.1], an additional list of standards can be of support:

- CEN EN 419 221-5 [i.31];
- CEN EN 419 241-1 [i.32];
- CEN EN 419 241-2 [i.33];
- ETSI TS 119 431-1 [i.34];
- ETSI TS 119 431-2 [i.35];
- ETSI TS 119 432 [i.36].

Annex B (informative): Bibliography

- ENISA: "Guidelines on supervision of qualified trust services; Technical guidelines on trust services", December 2017. ISBN: 978-92-9204-190-8. <https://www.enisa.europa.eu/publications/tsp-supervision>.
- ENISA: "Guidelines on termination of qualified trust services; Technical guidelines on trust services", December 2017. ISBN: 978-92-9204-244-8. <https://www.enisa.europa.eu/publications/tsp-termination>.

History

Document history		
V0.0.1	12.03.2018	Initial draft of the document.
V0.0.2	19.03.2018	Updated from “ESI-TSP audit - 319 403 supplements” meeting of 16.03.2018.
V0.0.3	02.04.2018	Updated from ESI-TSP mailing list comments.
V0.0.4	18.04.2018	Stable draft resulting from ESI#62.
V0.0.5	13.08.2018	Final draft updated from stakeholders’ comments.
V0.0.6	14.09.2018	Final draft updated from final stakeholders’ comments.
V0.0.7	02.10.2018	Final draft for public review