Introduction

Draft ETSI TS 119 403-3 v0.0.4 defines specific supplementary requirements for the application of ETSI EN 319 403 [REF-1] to conformity assessments (audits) of QTSP and the QTS they provide against the requirements of Regulation (EU) No 910/2014 [REF-2] assuming the use of ETSI policy requirement standards but not precluding use of other specifications.

In particular, the draft TS 119 403-3 defines requirements for conformity assessment reports (as specified in Regulation (EU) No 910/2014), including their content.

The ENISA technical guidelines on trust services “Guidelines on initiation of qualified trust services” [REF-3] have been used as basis for the draft TS 119 403-3.

Draft ETSI TS 119 403-3 v0.0.3 is provided as a stable draft as an indication of possible final content.

Collection of stakeholders input and comments

Stakeholders are kindly requested to provide comments on draft TS 119 403-3 and also input on any specific requirement they identify for the application of EN 319 403 [REF-1] to conformity assessments (audits) of qualified trust service providers and the qualified trust services they provide against the requirements of Regulation (EU) 910/2014 [REF-2].

Please download the template for comments and other inputs here: http://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc, and send your comments (in word format) **only** to E-SIGNATURES_COMMENTS@LIST.ETSI.ORG.

References

[REF-1] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[REF-2] 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.

[REF-3] ENISA: "Guidelines on initiation of qualified trust services; Technical guidelines on trust services", December 2017. ISBN: 978-92-9204-189-2.

https://www.enisa.europa.eu/publications/tsp-initiation

Draft ETSI TS 119 403-3 V0.0.4 (2018-04)

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

STABLE DRAFT

Download the template for comments:

https://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

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

by 8 June 2018

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

Copyright Notification

Contents

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 (CAB) performing certification of products, processes, or services. These requirements are not focussed on any specific application domain where CAB work.

In ETSI EN 319 403 [21] the general requirements of [i.30] are supplemented to provide additional dedicated requirements for CAB performing certification of trust service providers (TSP) 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 (NAB) as specified in Regulation (EC) No. 765/2008 [i.3] in applying ISO/IEC 17065 [i.30] for the accreditation of CAB that certify TSP 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 CAB performing certification of qualified trust service providers (QTSP) and the qualified trust services (QTS) they provide towards the requirements of Regulation (EU) No 910/2014 [i.1]. It aims supporting NAB for the accreditation of CAB 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 (QTSP) and the qualified trust services (QTS) they provide 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: "Conformity assessment -- Requirements for bodies providing audit and certification of management systems".

[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".

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
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

4 Requirements for CAB assessing QTSP/QTS against requirements of Regulation (EU) 910/2014

4.1 Conformity assessment scheme

CAS-4.1-01: The conformity assessment scheme for which a CAB is accredited to assess QTSP/QTS 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 fulfil requirements from Regulation (EU) No 910/2014 [i.1], include:

(a) Requirements on 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
(b) Control objectives and controls against which 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 conformity statement confirming - if such is the case - that the assessed QTSP/QTS meet all the applicable requirements of Regulation (EU) No 910/2014 [i.1], together with the list of those requirements.

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 the name of the NAB having accredited the CAB, and where applicable the registration number, as stated in the official records, the official postal address and electronic address of the NAB;

CAR-4.2-05: The CAR shall include the accreditation certificate or a link to the location of the accreditation certificate issued by the NAB referred to in CAR-4.2-04;

CAR-4.2-06: The CAR shall identify, when not mentioned in the accreditation certificate:

(a) the accreditation 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]).

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

CAR-4.2-07: The CAR shall include the accredited conformity assessment scheme document or a link to the location from where that document is available;

CAR-4.2-08: The CAR shall identify the name of the CAB responsible person having issued and signed the CAR;

CAR-4.2-09: 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;

CAR-4.2-10: The CAR shall identify, in accordance with clause 5.5.3 of ETSI TS 119 612 v2.1.1 [2] pursuant to CID (EU) 2015/1505 [i.2], the service digital identity(ies) of the QTS of the QTSP 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; and

(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 confirmation of conformity and on which criteria they can be identified;

CAR-4.2-11: The CAR shall provide for all QTS identified in CAR-4.2-10 a detailed description of the (e.g. PKI) functional architecture or hierarchy with the purpose to allow identification of the service(s) 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 CA illustrated in point (a), the list of the different types of certificates, identified by their service type identifier as defined in clauses 5.5.1 and 5.5.9.4 of ETSI TS 119 612 v2.1.1 [2] and by the criteria commonly identifying them 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].

CAR-4.2-12: Pursuant the conclusions of the conformity assessment, the CAR shall provide

(a) Either a confirmation that the corresponding content of the corresponding national trusted list [i.1], [i.2] do reflect the result of the assessment;

(b) Or a proposal or an indication for appropriate changes in the corresponding national trusted list [i.1], [i.2] that reflect the result of the assessment;

CAR-4.2-13: In line with CAR-4.2-11, the CAR shall include a precise and non-ambiguous summary of the QTS covered identifying which QTS components or service components are operated by third parties (e.g. subcontractors) indicating their name, where applicable registration number, as stated in the official records, official postal address and electronic address, as well as location of sites where the corresponding component services are operated;

NOTE 2: QTSP can make use of third parties, whether (Q)TSPs or not, to operate part or all of the components or component services 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 component services against its declared practices and policies as well as against Regulation (EU) No 910/2014 [i.1].

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) Subscriber agreements and related terms and conditions;

(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 maintains sufficient financial resources and/or has obtained appropriate liability insurance with regards to the provision of the QTS;

EXAMPLE 2: 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 and details about the underlying audit, evaluation, certification or assessment scheme;

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 importance, 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 15 regarding accessibility for person with disabilities;

(ii) Article 19.1 regarding risk based security due diligence;

(iii) Article 19.2 regarding security and personal data breach notification;

(iv) Article 23 on the correct use of the EU trust mark for qualified trust services, including provisions from CIR (EU) 2015/806 [i.8];

(v) 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 importance or include a reference to separately available audit reports in which such information is included;

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 3: 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: The CAR shall include, when the conformity is additionally confirmed or 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 importance;

CAR-4.2-20: The CAR shall detail the list of the third parties entrusted by the QTSP to perform all or parts of its processes supporting the provision of its QTS;

CAR-4.2-21: The CAR shall, in line with CAR-4.2-20, detail which of these third parties have been subject to the audit;

CAR-4.2-22: The CAR shall indicate:

(a) by when 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-4.2-23: The CAR shall indicate 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-4.2-24: The CAR should be protected in integrity and to ensure its origin either as being signed using the handwritten signature of the CAB responsible person, signed using an advanced electronic signature of the CAB responsible person sealed with an advanced electronic seal of the CAB, or protected by some equivalent method.

Annex A (informative): QTSP/QTS conformity assessment against Regulation (EU) 910/2014

A.1 Overview

Conformity assessment bodies (CAB) aiming to assess qualified trust service providers and the qualified trust services they provide (QTSP/QTS) against the requirements of Regulation (EU) 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 CAB 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 fulfil the requirements laid down in Regulation (EU) 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/QTS.

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 for each type of qualified trust service specified in [i.1] the list of relevant standards whose compliance is assumed to facilitate demonstration of compliance with requirements from [i.1]:

Table A.1: Standards available is 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], CAB 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 CAB, requirements on the auditing rules under which CAB 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.

CAB 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]), 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 (SB) 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 a qualified status.

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-initiation.
- 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-initiation.

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