EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Assessment of ETSI TS 119 403-3

Eligibility of ETSI TS 119 403-3 for referencing in an eIDAS implementing act

NOVEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use trust@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITOR

Ioannis Agrafiotis (ENISA), Slawomir Gorniak (ENISA)

AUTHORS

Olivier Delos (SEALED) and Sylvie Lacroix (SEALED)

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

TABLE OF CONTENTS

ABBREVIATIONS

CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CAS	Conformity Assessment Scheme
CEN	Centre Européen de Normalisation
CENELEC	European Committee for Electrotechnical Standardization
CID	Commission Implementing Decision
EA	European co-operation for Accreditation
EC	European Commission
EN	European Standard
ESO	European Standardisation Organisation
ETSI	European Telecommunications Standards Institute
ETSI TS	ETSI Technical Specifications
EU	European Union
ISO	International Organization for Standardization
MLA	Multilateral Agreement
NAB	National Accreditation Body
MS	Member State
QSCD	Qualified Signature/Seal Creation Device
QSigCD	Qualified Signature Creation Device
QSealCD	Qualified Seal Creation Device
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
SDI	Service Digital Identity
SB	Supervisory Body
TL	Trusted List
TS	Trust Service
TSP	Trust Service Provider
TSP/TS	Trust Service Provider and the Trust Service it provides

EXECUTIVE SUMMARY

Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market, introduced legal provisions at the EU level in relation to qualified trust service providers listed in the Regulation, and to the qualified trust services they provide. To acquire a qualified status, Trust Service Providers must demonstrate that they meet the requirements set in the eIDAS regulation by undergoing a compliance process. This process is conducted by an eIDAS accredited conformity assessment body (CAB) and results in a conformity assessment (audit) report.

The eIDAS Regulation does not specify an accreditation scheme or any conformity assessment (or certification) scheme against which a CAB must be accredited. This results in diverse conformity assessment schemes (CAS) used by CABs and influences the quality of the CARs provided by them. In order to harmonise this process, the European Commission can, by means of implementing acts pursuant to Art.20(4) of eIDAS, establish a number of reference standards regarding the accreditation of the CABs, the CAR, and the auditing rules under which CABs will carry out their conformity assessment of the QTSP/QTS.

A potential candidate for such a referencing pursuant to Art.20(4) is [ETSI TS 119 403-3], which sets additional requirements for CABs assessing EU QTSPs to those defined in [ETSI EN 319 403], which builds upon [ISO/IEC 17065] to specify requirements for CABs assessing Trust Service Providers. This document assesses the eligibility of [ETSI TS 119 403-3], and the standards it builds upon, to be referenced in an implementing act adopted pursuant to Art.20(4) of the eIDAS Regulation.

The findings suggest that if certain revisions take place, [ETSI TS 119 403-3] is a good and eligible candidate to be referenced in an implementing act adopted pursuant to:

- point (a) of Art.20(4) as it addresses both the accreditation of CABs and the content of the CAR, and
- point (b) of Art.20(4) as, by reference to [ETSI EN 319 403] (or preferably EN 319 403-1 when published and TS 119 403-3 being updated to reference it), it covers auditing rules under which the Conformity Assessment Bodies will carry out their assessments.

It is recommended that the European Commission requires ETSI to revise [ETSI TS 119 403-3] and [ETSI EN 319 403] to ensure that ETSI EN 319 403-1 is published, updating and correcting the current version of [ETSI EN 319 403]. It should be clarified whether ETSI EN 319 403 requires compliance with the entire set of requirements of ISO/IEC 17065 (e.g. unclear coverage of clause 6.1.3).

Furthermore, a potential update of [ETSI TS 119 403-3] would be beneficial to:

- require from an audit team of the accredited CAB to demonstrate knowledge of the eIDAS Regulation,
- cover Qualified Trust Service implementations that are not based on Public Key Infrastructure,
- require an eIDAS Conformity Assessment Scheme that will be in accordance to the [ISO/IEC 17067] guidelines

- include requirements on how component audit-reports are composed into the final Conformity Assessment Report.

Upon completion of these revisions, it is recommended that the European Commission refers in an implementing act adopted pursuant to Art.20(4) of eIDAS the combination of a set of standards including [ISO/IEC 17065] as the main accreditation framework, supplemented by ETSI EN 319 403-1 (as the successor and “correction” of the current [ETSI EN 319 403], see below), which itself is supplemented by [ETSI TS 119 403-3]. It is also suggested to add a reference to type 6 certification scheme as specified in [ISO/IEC 17067] for the development of an eIDAS Conformity Assessment Scheme.

1. INTRODUCTION

1.1 SETTING THE SCENE

Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market [eIDAS, 2014] (hereinafter eIDAS Regulation, or eIDAS), introduced legal provisions at the EU level in relation to qualified trust service providers (QTSPs) listed in the Regulation, and to the qualified trust services (QTSs) they provide (hereinafter collectively referred to as QTSP/QTSs).

A key policy choice made by the eIDAS Regulation is that, in order to be granted a qualified status and to be able to provide QTSs, trust service providers (TSPs) and the QTSs they intend to provide must first demonstrate that they meet the requirements of the eIDAS Regulation in relation to QTSP/QTSs. This implies that TSPs and the QTSs at hand need to undergo a specific process and receive formal approval from a competent national supervisory body (SB) to attest to their compliance. If successful, this process then leads to their inclusion in the national trusted list attesting their qualified status.

As part of this process, the prospective QTSP/QTS must be audited by an eIDAS accredited conformity assessment body (CAB) to confirm, through a conformity assessment (audit) report (CAR) that the QTSP and the QTS it provides meet the requirements of the eIDAS Regulation.

As a next step of the process, the prospective QTSP/QTS notifies its intention to provide QTS to its competent national supervisory body (SB) together with the positive CAR resulting from such an assessment. Taking the CAR into account, the SB will verify the conformance of the prospective QTSP/QTS to the eIDAS Regulation and will grant, or not, a qualified status.

The eIDAS Regulation does not specify any particular accreditation scheme or any conformity assessment (or certification) scheme against which a CAB must be accredited. This results in practice in a significant diversity regarding the conformity assessment schemes (CAS) used by CABs and influences the quality of the CARs provided by them.

In order to reduce this diversity, the European Commission may, by means of implementing acts pursuant to Art.20(4) of eIDAS, establish a number of reference standards regarding the accreditation of the CABs, the CAR, and the auditing rules under which CABs will carry out their conformity assessment of the QTSP/QTS.

A potential candidate for such a referencing pursuant to Art.20(4) is [ETSI TS 119 403-3], which sets additional requirements for CABs assessing EU QTSPs to those defined in [ETSI EN 319 403], which builds upon [ISO/IEC 17065] to specify requirements for CABs assessing TSPs.

1.2 SCOPE

The scope of this document is to assess the eligibility of [ETSI TS 119 403-3], and the standards it builds upon, to be referenced in an implementing act adopted pursuant to Art.20(4) of the eIDAS Regulation.

2. THE LEGISLATIVE FRAMEWORK

2.1 REGULATION (EU) N°910/2014 (eIDAS)

The eIDAS Regulation provides the regulatory framework for electronic identification and trust services for electronic transactions in the European digital market. One objective of this Regulation is to enhance the trust of enterprises and consumers in this market and to promote the use of trust services and products. To that end, the Regulation introduces the notions of QTS and QTSP, together with their requirements and obligations that ensure high-level of security of these QTSs and their associated products. When a TSP without qualified status intends to start providing QTS, or when a QTSP needs to confirm that the QTS it provides fulfils the eIDAS requirements and obligations, the QTSP shall be audited by a CAB.

The eIDAS Regulation reuses the definition of a CAB from [Reg.765/2008] (hereinafter Regulation (EC) N°765/2008), setting out the requirements for accreditation and market surveillance relating to the marketing of products. Regulation (EC) N°765/2008 defines a CAB as "*a body that performs conformity assessment activities including calibration, testing, certification and inspection*". In the context of the eIDAS Regulation, a CAB is a body as defined above that is additionally accredited as competent to carry out assessment of the conformity of a QTSP/QTS with the requirements of the eIDAS Regulation.

As a result of the audit performed, the CAB produces a CAR, which needs to confirm if the assessed (Q)TSP/QTS fulfils the requirements laid down in the eIDAS Regulation. This CAR should be submitted to the competent national SB, responsible for the supervisory tasks in the Member State in which the (Q)TSP is established. Based on this CAR, the SB verifies the compliance of (Q)TSP with the eIDAS requirements[1]. Upon positive decision of the SB, the QTSP/QTS is listed in the trusted list, attesting their qualified status.

The eIDAS Regulation does not specify any particular accreditation scheme, nor any CAS, against which a CAB must be accredited. Instead, the eIDAS Regulation simply requires the CAB to be accredited in accordance with Regulation (EC) N°765/2008 in order to ensure the accredited CAB is competent to carry out conformity assessment of a QTSP/QTS against the requirements of eIDAS Regulation.

2.2 REGULATION (EC) N°765/2008

Regulation (EC) N°765/2008 sets out the requirements for accreditation and market surveillance relating to the marketing of products. One of the purposes of this Regulation is to ensure the equivalence and the mutual recognition of the competence of CABs to carry out a specific conformity assessment activity, where this competence is attested by a national accreditation body (NAB). To that end, Regulation (EC) N°765/2008 has designated the European co-operation for Accreditation (EA)[2] to manage a peer evaluation system regarding the competence of NABs to evaluate the required competences of CABs. This mandatory peer-evaluation system facilitates the mutual recognition and promotes the overall acceptance of accreditation certificates and conformity assessment results issued by accredited bodies. National authorities shall recognise the equivalence of the services delivered by those accreditation bodies (i.e. the NABs) which have successfully undergone such peer evaluation,

[1] The competent SB has the final decision on the verification of such a compliance and on the initial grant of a qualified status to a (Q)TSP/QTS. The CAR submitted by the (Q)TSP is a pre-requisite to such a decision but might not be a sufficient condition. The SB may request further information and may take a duly justified decision that goes against the CAR.

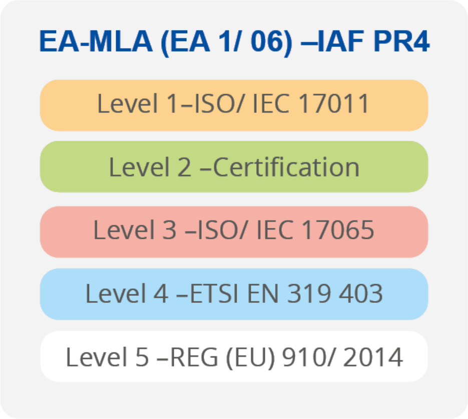
[2] https://european-accreditation.org

and thereby accept the accreditation certificates of those bodies and the attestations issued by the CABs accredited by them.

In line with the objective of ensuring the equivalence and mutual recognition of accredited CABs and of the conformity assessment attestations they issue, the EA has established a Multilateral Agreement (EA MLA), under which the signatories recognise the equivalence of each other's accreditation systems.

The EA has adopted the recommendation[3] to use an eIDAS accreditation scheme based on the [ISO/IEC 17065] accreditation framework, supplemented by [ETSI EN 319 403], as one possible route to demonstrate conformity with relevant requirements of the eIDAS Regulation through assessment by accredited CABs.

Figure 1: The EA recommended eIDAS CAB accreditation scheme



As illustrated in Figure 1, the eIDAS accreditation scheme recommended by EA requires:

- The accreditation of the CAB to be based on the [ISO/IEC 17065] certification framework;
- This [ISO/IEC 17065] accreditation framework of the CAB to be supplemented by [ETSI EN 319 403]. [ETSI EN 319 403] specifies additional dedicated requirements for CABs carrying out the certification of trust service providers and the trust services they provide, against defined criteria against which they claim conformance (those criteria being identified as the "Normative Document"); and
- The accreditation of the CAB to confirm the skills and competence of the CAB to conduct conformity assessment of QTSP/QTS against the requirements of the eIDAS Regulation, as being the Normative Document laying down criteria/requirements against which the QTSP/QTS conformance is to be assessed.

A specific characteristic of the eIDAS accreditation scheme recommended by the EA, and intrinsically of the eIDAS Regulation as Normative Document, is that the requirements against which the QTSP/QTS have to be certified are not technical requirements, but technology-neutral legal requirements expressed in terms of functional objectives. This is largely a continuation of the eIDAS Regulation's general policy preference for technical neutrality. The Normative

[3] EA Resolution 2014 (34) 22 and EA document EAGA(14)31: https://european-accreditation.org/wp-content/uploads/2018/10/34th-ea-ga-approved-resolutions-.pdf

Document is therefore not a technical standard but the QTSP/QTS applicable requirements from the eIDAS Regulation itself.

Neither the eIDAS Regulation nor the EA specifies the effective technical criteria or the technical certification scheme stemming from the provisions of the eIDAS Regulation. Furthermore, no standard is mandated, and no standard may be mandated, under the eIDAS Regulation, in relation to QTSPs or QTS to be granted a qualified status. QTSPs are free to implement any standard, or they may choose to implement no standard at all, provided they can demonstrate that the requirements of the eIDAS Regulation are met for both themselves and the QTS they provided.

Finally, no eIDAS secondary legislation has been adopted to date to reference any standard that would create a legal presumption of compliance with any requirements of the eIDAS Regulation for the QTSP/QTS that choose to adhere to it. However, even if such secondary legislation were adopted, compliance to such standards would still remain voluntary for QTSPs: they would remain free to use (or comply to) them or not.

It is worth noting that the EA recommended the eIDAS CAB accreditation scheme based on [ISO/IEC 17065] supplemented by [ETSI EN 319 403]. This is however, an EA recommendation and it is not mandatory. Each NAB signatory of the EA MLA may adopt the EA recommended scheme or use another scheme, provided that the alternative scheme is equivalent to [ETSI EN 319 403].

2.3 eIDAS ARTICLE 20.4 IMPLEMENTING ACT

Art.20(4) of the eIDAS Regulation gives the European Commission the competence, by means of implementing acts, to "*establish reference number of the following standards:*

a) accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;

b) auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1".

Where the Art.20(1) specifies:

> *"Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it."*

So far, no implementing act has been adopted pursuant to Art.20(4).

The current wording of Art.20(4) (i.e. "establish reference number of […] standards") does not allow the EC to profile the standards in order to amend standardised specifications in any appropriate way (i.e. it does not allow the EC to define the relevant specifications). At most, some of the requirements defined in a standard may be excluded from the reference in an implementing act. However, such exclusion mechanisms cannot be abused to *de facto* create specifications, which is not under EC mandate in the context of Art.20(4). So, when failures of candidate standards would be identified during their eligibility assessments for being referenced in accordance with Art.20(4), those failures would need to be notified to the competent standardisation organisations for updating the standards accordingly and republishing them.

2.3.1 Candidate standards for Art.20(4) referencing

Candidate standards for being referenced in an implementing act pursuant to Art.20(4) are scarce and include [ISO/IEC 17065], [ETSI EN 319 403] and the recently published [ETSI TS 119 403-3]:

- [ISO/IEC 17065] specifies requirements for CABs certifying products, processes and services. It is a generic framework applicable to any type of product, process, or service.
- [ETSI EN 319 403] builds upon and supplements [ISO/IEC 17065] to provide additional dedicated requirements for CABs performing certification of TSP/TS against defined criteria for which they claim conformance. It is agnostic against which type of criteria TSP/TS claim conformance with; it may be technical standards, publicly available specifications or regulatory requirements.
- [ETSI TS 119 403-3] has been recently published to further specify supplementary requirements to those defined in [ETSI EN 319 403] in order to provide additional dedicated requirements for CABs performing certification of QTSP/QTS conformity with the eIDAS requirements. In particular, it specifies suitability requirements for a CAS for which a CAB is accredited to assess QTSP/QTSs against eIDAS, and requirements on the content and scope of the resulting CAR.

However, it is worth noting that none of these standards fully specifies an eIDAS CAS. In particular, they are lacking the specification of a precise list of concrete criteria/controls, criteria/control objectives, checks and tests that an accredited CAB could use to carry out a conformity assessment of a QTSP/QTS with the eIDAS Regulation (cf. point (b) of Art.20(4)). No standard addressing such a list has been developed so far by (European) standardisation bodies. CEN/CENELEC and ETSI have, however, developed QTSP/QTS relevant best practices technical standards and even annexed tables mapping the requirements of the Regulation with the relevant clauses of these standards, but no formal assessment of their suitability has been performed so far, particularly with the aim of being referenced in an eIDAS implementing act.

The following sections provide an overview of the above candidate standards, focusing on [ETSI TS 119 403-3]; as this standard builds upon the two other candidates, it is the main focus of the this report.

3. ASSESSMENT & OPINION

3.1 INTRODUCTION

Since [ETSI TS 119 403-3] builds upon [EN 319 403], which in turn builds upon [ISO/IEC 17065], the present document intends to provide an opinion on the eligibility of [ETSI TS 119 403-3] to be referenced in an implementing act adopted pursuant to Art.20(4). For that to happen, the covered scope of this standard should be (partially or exhaustively) threefold:

A. **accreditation of the CAB**, in accordance with Regulation (EC) N°765/2008 and in a way that such accreditation ensures that the accredited CAB is competent to carry out conformity assessment of a QTSP/QTS against the requirements of eIDAS Regulation;
B. **content of the CAR** should contain a clear certification decision and sufficient information to respectively confirm and demonstrate that the assessed QTSP/QTS fulfils all the applicable requirements laid down in eIDAS Regulation. Therefore, CARs will effectively support the competent supervisory body in verifying if QTSP/QTS fulfil eIDAS requirements and decide whether to grant or not the qualified status to the assessed QTSP/QTS;
C. **auditing rules** under which the CAB will carry out its conformity assessment of the qualified trust service providers.

As can be observed in the list of currently notified eIDAS CABs[4], all of the 30 eIDAS CABs have been accredited under [ISO/IEC 17065]. For 28 of them, this framework is complemented by [ETSI EN 319 403]. For 2 of them, [ETSI EN 319 403] is not clearly indicated, although the corresponding CAB certification schemes claim to abide by [ETSI EN 319 403]. Very few, if any, of the 30 eIDAS CABs have asked their competent NAB to extend the scope of their eIDAS accreditation to include [ETSI TS 119 403-3]. Some of the SBs do require or strongly recommend QTSPs and the CABs assessing QTSP/QTS against eIDAS to provide a CAR that meets the requirements of [ETSI TS 119 403-3].

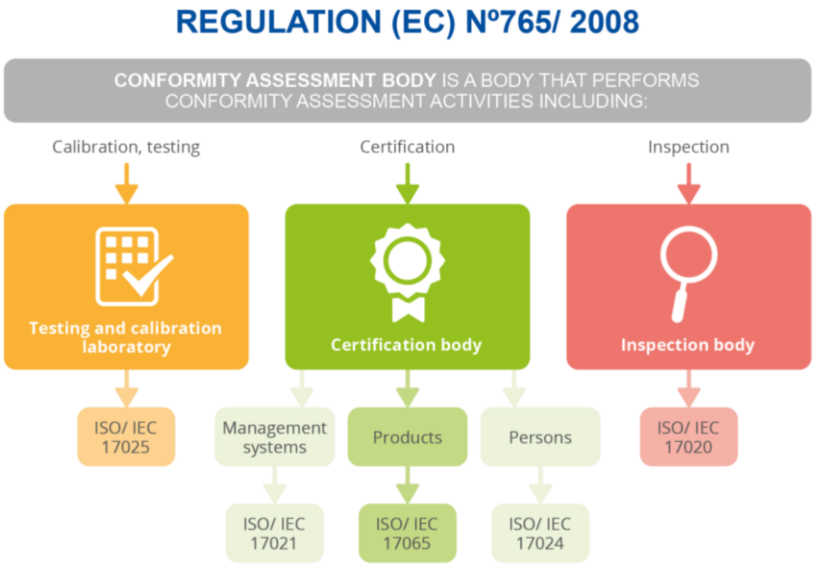
3.2 OVERVIEW OF ISO/IEC 17065

[ISO/IEC 17065] is an international standard that specifies requirements for bodies certifying products, processes and services. This standard intends to ensure that a certification body operates a certification scheme in a competent, consistent and impartial manner. It is worth noting that, as illustrated in Figure 2, this standard covers requirements for a subtype of conformity assessment bodies defined in Regulation (EC) N°765/2008[5], namely certification bodies. Hence, CABs accredited under this standard are certification bodies.

[4] Available at https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation

[5] Regulation (EC) N°765/2008 doesn't mandate the usage of any particular standard. The mapping between the Regulation and the ISO 170XX standards presented in the figure is for the sole purpose of illustration.

Figure 2: CABs in Regulation (EC) N°765/2008



As a framework, [ISO/IEC 17065] is agnostic to the scope of the certification and does not include CAB requirements related to TSP/TS or eIDAS.

3.3 OVERVIEW OF ETSI EN 319 403

[ETSI EN 319 403] is a European standard defining requirements for CABs which assess TSP/TS. As [ISO/IEC 17065] is not focused on the requirements of conformity assessment activities regarding specific types of products, processes or services, [ETSI EN 319 403] intends to provide additional dedicated requirements for CABs assessing TSP/TS against criteria for which they claim conformance.

To that end, the standard adopts the general requirements of [ISO/IEC 17065] to the specific context of the conformity assessment of TSPs. [ETSI EN 319 403] builds upon mandatory [ISO/IEC 17065]. It also adds further specific requirements mainly in terms of resources and on the assessment process. The ETSI standard also includes requirements related to the audit of a TSP's management system, as defined in [ISO/IEC 17021] and in [ISO/IEC 27006], either directly or by reference.

Compliance with [ETSI EN 319 403] de facto requires compliance with [ISO/IEC 17065]. However, formally [ETSI EN 319 403] does not require compliance with clause 6.1.3 (Contract with the personnel) from [ISO/IEC 17065], and does not require the CABs to be accredited against [ISO/IEC 17065]. This practice will likely have an impact on the referencing of [ETSI EN 319 403] in an implementing act adopted pursuant to Art.20(4). Therefore, it is recommended to refer to a set of standards including [ISO/IEC 17065] as the main accreditation framework, supplemented by [ETSI EN 319 403] (or its successor, see below), which is further supplemented by [ETSI TS 119 403-3].

[ETSI EN 319 403] is applicable to the assessment by CABs of all types of TSP/TS claiming compliance with any type of specifications. The standard is not specific to eIDAS and therefore can be seen as a generic standard regarding TSP/TS that may be reused (and is currently reused) as a basis for 3rd countries (i.e. non-EU) for defining “IAF MLA compliant” accreditation schemes for TSP/TS.

It is worth noting that the standard is currently under revision, in particular concerning the parts clarifying how pending non-conformities shall be handled by the CAB, clarifying certification decisions and adding guidance on determining audit time. The updated version is expected to be renamed [EN 319 403-1]. The current version of [ETSI EN 319 403] may be seen as problematic since it may be interpreted in a way that could give way to certification decisions with pending non-conformities.

As a general comment, the EA believes that [ISO/IEC 17065] supplemented by [ETSI EN 319 403] is the most appropriate track for accrediting CABs under eIDAS and for specifying rules under which CABs will carry out their conformity assessment of QTSP/QTS against the eIDAS Regulation as normative document.[6]

This track, however, does not cover any specific standardised requirements regarding the CAR resulting from such conformity assessments. [ETSI TS 119 403-3] fills this gap in the context of QTSP/QTS audited against the requirements of the eIDAS Regulation.

3.4 OVERVIEW OF ETSI TS 119 403-3

3.4.1 Scope

[ETSI TS 119 403-3] is part of a set of standards covering the TSP/TS conformity assessment. This set is composed of 3 parts:

1. Part 1: "Requirements for conformity assessment bodies assessing Trust Service Providers" now existing as [ETSI EN 319 403] but to be issued as Part 1 when revised;
2. Part 2: "Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates";
3. Part 3: "Additional requirements for conformity assessment bodies assessing EU qualified trust service providers" that is [ETSI TS 119 403-3], the standard presently analysed.

Complementing [ETSI EN 319 403] that provides generic requirements for CABs assessing any type of TSP/TS and is eIDAS-agnostic, [ETSI TS 119 403-3] specifies additional requirements for CABs assessing EU QTSP/QTS. Hence, the latter is focused only on the eIDAS context and on QTSP/QTS.

As a standard that is setting specific requirements for the assessment of QTSP/QTS, [ETSI TS 119 403-3] has two objectives:

1. Specify supplementary requirements to those defined in [ETSI EN 319 403];
2. Support NABs for the accreditation of CABs in line with Art.3(18) of the eIDAS Regulation.

The specifications on QTSP/QTS’ CARs, aiming to confirm the compliance of the assessed QTSP/QTS with the requirements of the eIDAS Regulation, will also potentially support SBs required to verify conformity before granting qualified status.

[6] The EA rationale for selecting ISO/IEC 17065 & ETSI EN 319 403 as the CAB accreditation framework for TSP/TS assessments, and disregarding the ISO/IEC 17020, 17021 and 27006 tracks, is described in “ENISA Guidelines on Initiation of Qualified Trust Services”. It is reproduced in Annex A for the ease of the reader.

3.4.2 Content

The normative requirements specified by the [ETSI TS 119 403-3] standard are divided into two main clauses:

- Clause 4.1 specifying requirements on the "Conformity assessment scheme", and
- Clause 4.2 specifying requirements on the "Conformity assessment report".

Requirements in [ETSI TS 119 403-3] are numbered using CAS-4.1-x or CAR-4.2-y respectively, where "x" and "y" are numbers. The following sections are referring to requirements using the same notation.

3.4.2.1 Conformity assessment scheme

CAS-4.1-01 first specifies that the CAS for which a CAB is accredited to assess QTSP/QTSs against the requirements of eIDAS Regulation in accordance with Regulation (EC) N°765/2008

"*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* [eIDAS] *Regulation".*

This requirement ensures that the accreditation of the CAB conforms with the eIDAS definition of a CAB (cf. Art.3(18)).

There is no requirement regarding the entity that defines the CAS. However, the informative Annex A of [ETSI TS 119 403-3] mentions that such a CAS can be defined by the CAB itself, by a competent EU SB, or by any other body possessing the necessary technical competence.

CAS-4.1-02 specifies that the CAS *shall, with the aim of confirming that the assessed QTSP/QTS fulfils the applicable requirements from* [the eIDAS] *Regulation, include:*

a) 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;[7] *and*

b) control objectives and controls against which the CAB will assess a QTSP/QTS against the applicable requirements of [the eIDAS] *Regulation.*

As detailed in the note above, the CAB shall comply with [ETSI EN 319 403]. This conformance implies that the CAB will also be compliant with [ISO/IEC 17065] rendering it a certification body. Therefore, in the case where [ETSI TS 119 403-3] is made mandatory in eIDAS, it will oblige eIDAS CABs to become certification bodies and exclude the other types of CABs as defined in Regulation (EC) N°765/2008 (i.e. testing and calibration laboratories and inspection bodies).

Additionally, this statement adds as a requirement that the CAS shall contain control objectives and controls when assessing the QTSP/QTS. As stated in the beginning of the sentence of **CAS-4.1-02** and as it is detailed in clause 4.2 from [ETSI TS 119 403-3], these audit controls and controls' objectives shall target the specific requirements of the assessed QTSP/QTS as defined in eIDAS.

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

The last requirement of this clause, **CAS-4.1-03**, is a normative reference to the next clause, i.e. clause 4.2 of [ETSI TS 119 403-3], specifying the requirements on eIDAS CARs.

3.4.2.2 Conformity assessment report

CAR-4.2-01 indicates that the issued CAR shall clearly indicate the decision of the CAB regarding the conformance of the QTSP/QTS with eIDAS requirements. In order to justify this decision, the CAR shall provide (**CAR-4.2-02**) sufficient details to demonstrate that the assessed QTSP/QTS meet all applicable requirements laid down in eIDAS Regulation. Starting from **CAR-4.2-03**, this clause of the standard presents requirements about the minimum content of the conformity assessment report, namely:

- Information to explicitly identify
  - the CAB that issued the CAR together with its CAS (CAR-4.2-03),
  - the NAB that accredited and is currently supervising this CAB, and
  - further information regarding the latter accreditation (CAR-4.2-04);
- Information about the assessed QTSP: CAR-4.2-08 implicitly adds as a requirement the fact that the CAR shall only cover one QTSP. This QTSP may make use of third parties, for whom it shall provide an exhaustive list and detailed information on which QTS components or service components they provide/operate.
- Identification of the service of digital identities and the associated PKI hierarchy (CAR-4.2-09 and 10). This sets as a mandatory requirement the use of PKI when providing a qualified trust service. This requirement may therefore be seen as conflicting with the technology neutrality of eIDAS or at least does not cover cases where the QTS provided is not based on PKI technology. This matter is further discussed in 3.5.4.2 Section 2.
- Indication on the content of TL, in case the qualified status is granted to the assessed QTSP/QTS. CAR-4.2-11 does not clarify who should provide the detailed description of this indication. In any case (whether this indication is provided by the QTSP or by the CAB), the CAB shall verify the veracity of this indication. Verifying the correctness of this indication therefore requires a good knowledge of [TS 119 612]. Demonstrating knowledge of [TS 119 612], and in general of eIDAS and its secondary legislation, is a requirement not explicitly present in this standard and probably implicitly covered by [ETSI EN 319 403] (cf. clause 6.2.1.8 of that standard).
- Evaluation report with indication of non-conformities with eIDAS requirements (CAR-4.2-16). The coverage of this eIDAS requirement is further analysed in Section 3.5.4.
- Information about the audit itself (e.g. detailed audit controls and control objectives, test samples, efforts and period of the audit) and the next surveillance audits (CAR-4.2-15, CAR-4.2-17 to CAR-4.2-21).
  - The required documentation (CAR-4.2-05, CAR-4.2-06, CAR-4.2-12 to CAR-4.2-14).
  - An explicit statement that the certification documents, including the CAR, are also intended for use by SBs (CAR-4.2-22).
- One or more qualified electronic signatures on the CAR, created by the CAB responsible person(s) having authorized the certification decision (CAR-4.2-07).

3.5 OPINION ON THE ELIGIBILITY OF TS 119 403-3 FOR REFERENCING

This section provides an opinion regarding both the content of [ETSI TS 119 403-3] and its eligibility for being referenced in an implementing act adopted pursuant to Art.20(4) of eIDAS.

3.5.1 eIDAS Specific

As presented above in Section 3.3, [ETSI EN 319 403] is eIDAS-agnostic. If an implementing act is to be issued in relation with eIDAS Art.20(4) for designating reference number of standard(s), [ETSI TS 119 403-3] is a more appropriate candidate than [ETSI EN 319 403] as it provides additional requirements for CABs assessing EU QTSP/QTS, namely requirements on the related CAS and CAR. Considering the current situation where SBs experience diversity in the scope and quality of the CAR, where stakeholders experience variety in the content and quality of the CAS, specifying further requirements in these respects in addition to [ETSI EN 319 403] is essential; provided these additional requirements are assessed to be suitable for supporting the eIDAS requirements.

It is worth mentioning that one of the key benefits of the eIDAS Regulation is to establish a clear and EU-wide legal effect of QTS outputs (e.g. Art.25(3) for qualified electronic signatures, Art.35(3) for qualified electronic seals, and Art.41(3) for qualified timestamps). In this respect, it is of paramount importance to ensure that QTSP/QTS requirements are consistently applied throughout Europe. Any progress in this direction can only improve confidence in trustworthiness and acceptability of QTS.

3.5.2 Version of the standard

[ETSI TS 119 403-3] currently refers to [ETSI EN 319 403]. As already mentioned, the latter is planned to be updated soon, with revisions addressing important corrections and clarifications regarding handling of non-conformities and certification decisions by the CABs. Practices currently vary across CABs on how to handle non-conformities irrespectively of their size and importance. The updated standard is planned to address this issue (among other minor corrections).

[ETSI TS 119 403-3] currently refers to [ETSI EN 319 403] without referring to any explicit versioning number of the latter. As stipulated in clause 2.1 of the standard (and as a general practice in ETSI standards), for non-specific references (i.e. without the mention of the version number), the latest version of the referenced document applies. [ETSI TS 119 403-3] would then “automatically” refer to the updated version of [ETSI EN 319 403] as soon as the latter is published.

The updated [ETSI EN 319 403] is, however, planned to be renamed to “ETSI EN 319 403-1” to better fit in a “x19 403-x” series. As a consequence, [ETSI TS 119 403-3] will have to be updated accordingly to refer to this new “ETSI EN 319 403-1”, leading to an updated version number of [ETSI TS 119 403-3] as well. As reference numbers of standards designated in eIDAS are commonly fixed versions (e.g. CID 2015/1506, CID 2015/1505, CID 2016/650), referencing [ETSI TS 119 403-3] in Art.20(4) shall follow the completion of ETSI’s updated version.

3.5.3 CAS requirements

[ETSI TS 119 403-3] includes two requirements on the CAS (there is an additional reference about the CAS output, i.e. the CAR).

Requirement **CAS-4.1-01** states that the CAS for which the CAB is accredited shall be defined in a way that such accreditation ensures that the CAB is competent for performing assessment of QTSP/QTS against eIDAS.

This requirement clearly reflects eIDAS Art.3(18) which defines a CAB as *"a body defined in point 13 of Art.2 of Regulation (EC) N°765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides".*

CAS-4.2-02 specifies requirements on the CAS content. To be compliant with [ETSI TS 119 403-3], a CAB shall use a CAS that contains:

- Requirements on the CAB:
  - meeting at least requirements of [ETSI EN 319 403] (so that [ETSI TS 119 403-3] mandates [ETSI EN 319 403], and also designates the CAB to become a certification body);
  - requirements on the auditing rules and on the set of criteria.
- Control objectives and controls used by the CAB for the assessments of QTSP/QTS against eIDAS.

Neither of these requirements mandate, specify or provide detailed guidance for the actual content of a CAS (no template, no general structure, no table of content are proposed) in a way similar to [ISO/IEC 17067], which provides guidelines for product (service) certification schemes. To this extent, it is recommended that:

- [ETSI TS 119 403-3] is amended to require the eIDAS CAS to be developed in accordance with the guidelines of [ISO/IEC 17067], and in particular as a type 6 certification scheme as defined in clause 5 of the ISO standard; and/or
- The implementing act adopted pursuant to Art.20(4) will refer to [ISO/IEC 17067] and in particular to its type 6 certification scheme.

Despite the peer review mechanism between NABs operating under Regulation (EC) N°765/2008, there is little assurance on the quality of the CASs used by the CABs for the assessment of QTSP/QTS against the eIDAS requirements. Referencing [ETSI TS 119 403-3] in an Art.20(4) implementing act would be a first step in harmonizing these CASs. However, complementary, and significant work should be planned for the development of an EU harmonized eIDAS CAS. This work should focus on the design of a certification scheme regarding the assessment of the conformity of QTSP/QTS, for each of the nine types of QTS specified in eIDAS, defining in particular the list of checks, evaluation criteria, evaluation criteria objectives, tests, etc. to be used by eIDAS accredited CABs to confirm the conformity of the assessed QTSP/QTS with the eIDAS requirements[8].

3.5.4 CAR requirements

As already stated above, SBs experience differences in the general assessment approach of CABs, and in the scope and quality of the resulting CARs. Because of its pivotal in the decision of the SB, the quality, reliability, and exhaustiveness of the content of the CAR are of paramount importance.

As most CABs are certification bodies, they might be issuing an assessment report that is targeting the requester only, instead of a CAR (as is the case of eIDAS) being primarily aimed for a third-party (i.e. the SB), who requires detailed input and justification for taking an informed final decision on whether to grant a qualified status. By enforcing an explicit declaration that the CAR is intended for the use by SBs, **CAR-4.2-22**, might partly or indirectly address this concern.

[8] For further information see the ENISA "Towards a harmonised Conformity Assessment Scheme for QTSP/QTS".

These SB requirements shall be escalated and emphasized to the NABs when accrediting CABs. Clause 4.2 from [ETSI TS 119 403-3] sets requirements clarifying expected content of an eIDAS CAR. The main elements of these requirements are discussed in the following sub-sections.

3.5.4.1 Clear identification

CAR-4.2-01 to **CAR-4.2-08** lists general but essential requirements on identification of:

- Clear formulation of the certification decision from the CAB;
- The identity of the CAB;
- The identity of the NAB;
- Both the corresponding accreditation scheme and the CAS[9];
- The signature(s) of the CAR (via EU qualified electronic signature(s)) to identify the CAB responsible person(s) who authorizes the certification decision;
- The identity of the QTSP and any other entity(ies) involved in the provision of the QTS and hence in the scope of the certification decision.

CAR-4.2-20 requires the CAB to indicate the dates of the next surveillance audit (when applicable) and of the next compliance audit. These elements translate good practices in documenting the decision with appropriate context.

CAR-4.2-02 requires the CAR to provide sufficient details to demonstrate the fulfilment of the eIDAS requirements. “Sufficient details” should be further elaborated, as **CAR-4.2-16** also refers to the conformity to the eIDAS requirements. From the provided note, the intent of this requirement is to ask for the reference and provision of any report (e.g. audit report against a standard) or documentation (e.g. practices, policies). The latter is however covered in **CAR-4.2-14**. This clause shall be clarified further, in particular in the light of specific but frequent processes such as composite audits (see below).

3.5.4.2 Trusted list content

CAR-4.2-09 to **CAR-4.2-11** cover important requirements for the content of the CAR in preparation of the corresponding trusted list service-entries.

These requirements address the identification of the service digital identity(ies) (SDIs) in accordance with the trusted list standard [ETSI TS 119 612] on which [CID 2015/1505] builds the specifications for EU MS trusted lists. The correct identification of these SDIs is indeed essential for the future listing of the service entries in the national trusted list, as they will determine the correct validation of QTS outputs against the content of the trusted list (e.g. the validation of a qualified timestamp issued by a QTS of the trusted list, or the validation of qualified electronic signature based on a qualified certificate issued by a QTS in that list).

These requirements also address, when applicable (i.e. in certain cases of issuance of qualified certificates) the important identification of sets of certificates that might require qualifications extensions as defined in clause 5.5.9.2 of [ETSI TS 119 612].

Although very useful for the preparation of the content of the trusted list, this part of [ETSI TS 119 403-3] is not however technology agnostic, but clearly PKI-based, with no alternative proposed for QTSP/QTS that would not use PKI technology. For its inclusion in an accreditation scheme, and more importantly for its referencing in an Art.20(4) implementing act, it is recommended that [ETSI TS 119 403-3] is updated to address such a concern. Therefore, it

[9] CAR-4.2-06 may seem sufficient compared to CAR-4.2-04 c) ii) as the former provides the content of the CAS while the latter requires only to specify the identity of it.

should cover non-PKI based implementations of QTS, as these are already covered by TS 119 612 clause 5.5.3 referenced in **CAR-4.2-09** of TS 119 403-3.

3.5.4.3 Demonstration of compliance with eIDAS requirements

One of the core requirements of [ETSI TS 119 403-3] regarding the content of the CAR is **CAR-4.2-16** where the CAR is required to contain content demonstrating the fulfilment of each applicable eIDAS requirement.

Both general requirements for QTSP/QTS, and specific requirements for each provided QTS are explicitly listed in this clause. Listing explicitly all nine types of QTS, and corresponding applicable eIDAS requirements certainly clarifies the scope of the assessment, and helps harmonization among CABs' approaches and CARs' contents, in a current situation where SBs experience too much variation in these respects.

In addition, **CAR-4.2-17** asks for a detailed description of the controls objectives and controls that have been conducted during the audit. This is certainly an important input in order for the SB to understand "how well and detailed" the assessment has been performed. This actually is commonly referred to as "evaluation reports".

3.5.4.4 Composite audits

A strong tendency in the EU (Q)TSP market is the specialization of third parties in the provision of parts (or components) of a trust service, commonly referred to by the term "service components" (e.g. in ETSI x19 xx1 standards on TS/components requirements). This term is used to illustrate the fact that these components are not trust services per se, but are delegated by TSPs to specialized entities. TSPs may then rely on these service components for part or all of their activities, bearing the final liability on the resulting consolidated trust service. Examples of such service components include: registration activities for certificate issuance, QTS factory services (e.g. "CA factory" activities outsourced for the issuance of certificates), alternative identification methods under eIDAS Art.24(1)d (e.g. remote identification, video identification).

The remote QSCD operation and management by a QTSP (cf. Annex II.3 of eIDAS) is not strictly speaking considered as a QTS service component but may be considered as a specific target of evaluation or assessment in the context of the supervision of such QTSP activities by a SB; in particular when a SB would require an ad-hoc conformity assessment (cf. Art.20(2) of eIDAS). This topic is addressed in a separate section below.

[ETSI TS 119 403-3] specifies in requirement **CAR-4.2-02** that the CAR shall provide sufficient details to demonstrate the fulfilment of eIDAS requirements. However, guidance or requirements on how component audit-reports are composed into the final CAR would be welcomed in order to ensure that the appropriate level of information reaches the SB. In particular:

- When the component audits have been performed;
- The duration of the validity of these component audits, and how this may affect the validity of the CAR;
- Even more important and more subject to ambiguity, on which scope the component audit has been performed and which assurance can be provided that this scope covers the present QTS under assessment. Component services may be audited as a generic service, which may then be instantiated and provided to several clients[10]. Defining how far this initial generic scope covers the particular instantiation for a

[10] A problematic case would be that the component service has actually been audited on a specific instantiation, unrelated to the QTS under assessment, and not in a generic context.

specific client is essential (e.g. the case of an audited generic CA factory, later duplicated in a specific instance for specific QTSP/QTS issuing qualified certificates, with potentially a dedicated CA hierarchy, a root CA key ceremony).

[ETSI TS 119 403-3] requirement **CAR-4.2-08** states that the CAR shall identify the contractors that operate trust-service components in scope. Linking this identification with **CAR-4.2-02** would benefit the readability of the CAR.

3.5.4.5 Remote QSCD operation and management

The particular case of remote QSCD supervision is not clearly addressed in [ETSI TS 119 403-3]. A remote QSCD (i.e. a QSCD managed on behalf of the user by a QTSP) shall be compliant to the applicable eIDAS requirements. As identified in the recent ENISA report [ENISA rQSCD], this remote QSCD, to the contrary of a local QSCD, is not only subject to certification but its operation is also subject to supervision by the SB. In particular regarding those requirements pointed in Annex II.3 & 4 of eIDAS.

According to [ENISA rQSCD] clause 5.1 page 28, “A certified QSCD can only be officially recognised as such once the QTSP has been duly supervised to manage the QSCD according to requirements and assumptions on the environment provided in the PPs”. This tends to be confirmed by the list of QSCDs compiled by the EC[11]. The EC list states that devices, which are managed on behalf of the user (signatory/seal creator) by a QTSP, can be only considered as QSigCD/QSealCD when they are duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.

Remote QSCD operation and management is not identified as a QTS under eIDAS. One may argue that it is not a trust service component either, in the sense of an activity outsourced by a QTSP for the provision of a QTS. These activities are within the boundaries of a “qualified signature creation device” and indeed are not consideredas a trust service[12] nor as a qualified trust service.

However, since these Annex II.3 activities may only be performed by QTSPs, it is also likely that QTSPs, who generate and manage electronic signature (seal) creation data on behalf of the signatory (creator of the seal) in the context of Annex II.3 (and II.4), would be required to meet the applicable requirements of eIDAS with regards to such activities. These applicable requirements may include all QTSP related requirements in eIDAS that are not specific to the provision of a QTS (e.g. Art.5, Art.13, Art.15, points (b), (c), (e), (f), (g), (h), (i) and (j) of Art.24(2)).

It can be further argued that the regular Art.20(1) and ad-hoc Art.20(2) audit activities, hence the related conformity assessment reports, cover the activities of QTSPs in the context of Annex II.3/4.

Since [ETSI TS 119 403-3] aims to further specify the requirements of [ETSI EN 319 403] regarding conformity assessments (audits) of (Q)TSP/QTS against the requirements of eIDAS, the assessment of QTSP activities in the context of Annex II.3 should logically fall in the scope of that standard as well.

[11] https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds
[12] Annex II.3 addresses the “generation” and “management” of signature creation data (i.e. private signing key) and does not address the creation of electronic signature, on behalf of the signatory.

Considering the ambiguity under eIDAS related to the status of the remote QSCD operation and management, and the criticality of its effective supervision, it is suggested to update[13] [ETSI TS 119 403-3] to separately address requirements on eIDAS CAR, regarding the results of the assessment of Annex II.3/4 activities by QTSP against the applicable requirements of the eIDAS Regulation.

3.5.4.6 Test results

CAR-4.2-18 of [ETSI TS 119 403-3] requires CABS to include in the CAR the description and the result of the set of tests or production samples and the assessment of the QTS output(s).

Together with **CAR-4.2-16** and **CAR-4.2-17**, it is indeed crucial for the SB to understand how the assessment of the CAB has been performed. As cited by [ETSI TS 119 403-3], certain types of QTS, such as the qualified validation of qualified electronic signature, cannot be reliably assessed on the basis of just examining a few samples. In the case of qualified validation of qualified electronic signature, [ETSI TS 119 615] and [ETSI TS 119 172-4] have shown that there exist more than 100 variations of cases depending on the certificate content, trusted list content, pre/post-eIDAS time of signing, etc. More testing facilities exist, such as conformance checkers from ESOs, or EC CEF building blocks reference implementations or testing facilities; those facilities may/should be leveraged to ensure a reliable outcome for the audit report.

3.5.5 Referencing ETSI TS 119 403-3 and Coverage of Art.20(4)

For the reasons described above, [ETSI TS 119 403-3], or preferably its recommended updated version, can be seen as a good and eligible candidate for being referenced in an implementing act adopted pursuant to

- point (a) of Art.20(4) as it addresses both the accreditation of CABs and the content of the CAR, and
- point (b) of Art.20(4) as by reference to EN 319 403 (or preferably EN 319 403-1 when published and TS 119 403-3 being updated to reference it) Art.20(4) covers auditing rules under which the CABs will carry out their assessments.

It is worth noting that none of the [ISO/IEC 17065], [ETSI EN 391 403] or [ETSI TS 119 403-3] specify a standardized eIDAS conformity assessment (certification) scheme (i.e. a detailed list of criteria/control and criteria/control objectives against which the QTSP/QTS shall be assessed to confirm they meet the requirements of eIDAS). The eIDAS Regulation remains the normative document (Level 5 in Figure 1) against which the QTSP/QTS must be assessed.

CEN/CENELEC and ETSI have produced a wide set of standards to facilitate CABs in demonstrating and certifying QTSP/QTS compliance with the applicable requirements of eIDAS, as illustrated in Table A.1 of Annex A of [ETSI TS 119 403-3]. However, so far none of these standards has been formally assessed for being eligible to support such a demonstration of compliance. 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 the QTSP/QTS requirements laid down in eIDAS. The eIDAS Regulation does not even foresee such secondary legislation for all the requirements applicable to QTSP/QTSs.

The level of flexibility given by [ETSI 119 403-3] to CABs to design or use a conformant CAS may be the right approach. Mandating the use of specific TSP/TS related standards (e.g. as

[13] As a side note not related to composite audits but only to QSCD when used by a QTS for the provision of qualified certificates for electronic signatures or seals, CAR-4.2-14 iv) refers to the list of QSCDs "when the (Q)TSP delivers such devices to its users", where actually there is no QSCD delivered in the case of remote QSCD. Even in the case of local QSCD, it may be argued that the statement is ambiguous. As stated in ETSI EN 319 411-2: whether the device is prepared by the TSP or not, the TSP shall verify that the device is certified as a QSCD. The (Q)TSP may not deliver such devices but would still need to provide the list of QSCD.

listed in Table A.1 of [ETSI TS 119 403-3]) is not possible towards QTSPs. Mandating the use of such standards by eIDAS accredited CABs to build their eIDAS conformant CAS would not be recommended without a formal assessment of the eligibility of such standards to support demonstration of QTSP/QTS compliance with eIDAS. The end-result would likely be reducing the innovation from QTSPs. Mandating the use of standards may also not be applicable/suitable in all types of QTS implementation, and may lead to confusion with regards to CABs and QTSPs as in no case compliance with such standard may be required.

3.5.6 Legal effect of an Art.20(4) implementing act

The legal effect of the referencing of standard(s) under Art.20(4) shall be clarified. Establishing “reference number of […] standards” may:

- Either have a mandatory effect where all CABs shall be compliant to [ETSI TS 119 403-3], [ETSI EN 319 403] and [ISO/IEC 17065], or
- Establish one possible path for conformity.

The benefit of both cases would be to establish some sort of harmonization, in stark contrast to the current situation. Strongest harmonization would be achieved using option 1, because of its mandatory nature.

The current approach of the EA rules to allow EA MLA signatories to freely choose between implementing the EA recommended eIDAS accreditation scheme or using alternatives (provided these have been evaluated as being equivalent) may be considered within the context of the adoption of an implementing act pursuant to Art.20(4) of eIDAS. Any scheme that would be an alternative to the combination of [ISO/IEC 17065], [ETSI EN 319 403], [TS 119 403-3] and [ISO/IEC 17067] type 6 certification scheme requirements, would be authorised as well; provided that such scheme is evaluated as equivalent to EA recommendations and the demonstration of equivalence is assessed as part of the peer-review management in line with Regulation (EC) N°765/2008.

4. CONCLUSIONS

This report assessed the eligibility of [ETSI TS 119 403-3], and the standards it builds upon, to be referenced in an implementing act adopted pursuant to Art.20(4) of the eIDAS Regulation.

Provided that certain revisions take place, [ETSI TS 119 403-3] is a good and eligible candidate to be referenced in an implementing act adopted pursuant to:

- point (a) of Art.20(4) as it addresses both the accreditation of CABs and the content of the CAR, and
- point (b) of Art.20(4) as, by reference to [ETSI EN 319 403] (or preferably EN 319 403-1 when published and TS 119 403-3 being updated to reference it), it covers auditing rules under which the CABs will carry out their assessments.

Nonetheless, in this context of adopting an implementing act pursuant to Art.20(4) of the eIDAS Regulation, it is recommended to the European Commission to first require ETSI to revise [ETSI TS 119 403-3] and [ETSI EN 319 403]:

- To ensure ETSI EN 319 403-1 is published updating and correcting the current version of [ETSI EN 319 403], in particular with regards to the handling of non-conformities and to the certification decisions. As part of the revisions, it should be clarified whether ETSI EN 319 403 requires compliance with the entire set of requirements of ISO/IEC 17065 (e.g. unclear coverage of clause 6.1.3).
- To update [ETSI TS 119 403-3], in order:
  - To refer to ETSI EN 319 403-1 updating [ETSI EN 319 403]
  - To require the audit team of the accredited CAB (e.g. in addition to the requirements specified in [ETSI EN 319 403], or its successor, in particular in its clause 6.2.1.8) to demonstrate knowledge of the eIDAS Regulation, including the secondary legislation with regards to trust services(in particular of the implementing act adopted pursuant to Art.22(5), which defines the technical specifications and formats for trusted lists)
  - For CAR-4.2-09 and CAR-4.2-10 to cover QTS implementations that are not based on PKI technology, and/or for which no PKI-based SDI is applicable; as it is already foreseen in EU MS Trusted Lists and in [ETSI TS 119 612] clause 5.5.3 referenced by these requirements
  - To require the eIDAS CAS to be developed in accordance with the guidelines of [ISO/IEC 17067], and in particular as a type 6 certification scheme as defined in clause 5 of the standard
  - To include guidance or requirements on how component audit-reports are composed into the final CAR in order to ensure the appropriate level of information of the SB
  - To link CAR-4.2-02 with the identification in CAR-4.2-08 of contractors that operate trust-service components
  - To separately address requirements on eIDAS CAR, regarding the results of the assessment of Annex II.3/4 activities by QTSP against the applicable requirements of the eIDAS Regulation.

Upon completion of these revisions, it is recommended that the European Commission refer (in an implementing act adopted pursuant to Art.20(4) of eIDAS) to the combination of a set of standards including [ISO/IEC 17065] as the main accreditation framework, supplemented by

ETSI EN 319 403-1 (as the successor and “correction” of the current [ETSI EN 319 403], see below), which itself is supplemented by [ETSI TS 119 403-3]. It is also suggested to add a reference to type 6 certification scheme as specified in [ISO/IEC 17067] for the development of an eIDAS CAS.

The implementing act should be adopted in a manner that will not prohibit the use of, or will explicitly allow any alternative to the combination of [ISO/IEC 17065], ETSI EN 319 403-1, [ETSI TS 119 403-3] and [ISO/IEC 17067] type 6 certification scheme requirements. It should, however, be required that for such an alternative to be eligible, it must be evaluated as equivalent to the referenced combination of standards and the demonstration of equivalence should be assessed as part of the peer-review management in line with Regulation (EC) N°765/2008.

Finally, it is recommended that the European Commission clarify, when possible, the (legal) consequences of referring to standards by means of an implementing act adopted pursuant to since Art.20(4) of the eIDAS Regulation.

5. BIBLIOGRAPHY/REFERENCES

5.1 REFERENCES

ID	Description
eIDAS, 2014	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
ENISA, 2015	Analysis of standards related to Trust Service Providers Mapping of requirements of eIDAS to existing standards. July 01, 2016. https://www.enisa.europa.eu/publications/tsp_standards_2015
ETSI EN 319 403	ETSI EN 319 403 V2.2.2 (2015-08): "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".
ETSI TS 119 403-3	ETSI TS 119 403-3 V1.1.1 (2019-03): "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers".
ETSI EN 319 401	ETSI EN 319 401 V2.2.1 (2018-04): "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
ETSI EN 319 411	ETSI EN 319 411 (2018-04): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1 (V1.2.2): General requirements; Part 2 (V2.2.2): Requirements for trust service providers issuing EU qualified certificates".
ETSI EN 319 421	ETSI EN 319 421 V1.1.1 (2016-03): "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
ISO/IEC 17021	ISO/IEC 17021:2017: "Conformity assessment -- Requirements for bodies providing audit and certification of management systems".
ISO/IEC 17025	ISO/IEC 17025:2017: "General requirements for the competence of testing and calibration laboratories".
ISO/IEC 17065	ISO/IEC 17065:2012: "Conformity assessment -- Requirements for bodies certifying products, processes and services".
ISO/IEC 17067	ISO/IEC 17067:2013: "Conformity assessment -- Fundamentals of product certification and guidelines for product certification schemes".
ISO/IEC 27006	ISO/IEC 27006:2015: “Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems”
Reg.765, 2008	Regulation (EC) 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. OJ L 218, 13.8.2008, p. 30–47. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008R0765&amplocale=en
ENISA rQSCD	Assessment of Standards related to eIDAS. Recommendations to support the technical implementation of the eIDAS Regulation. November 2018
CID 2015/1505	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

CID 2015/1506	Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(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
CID 2016/650	Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) 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
ETSI TS 119 612	ETSI 119 612 v2.1.1: “Electronic Signatures and Infrastructures (ESI); Trusted Lists”
ETSI TS 119 615	ETSI TS 119 615: “Electronic Signatures and Infrastructures (ESI); Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists”
ETSI TS 119 172-4	ETSI TS 119 172-4: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists”

ANNEX A

A.1 EA RATIONALE FOR SELECTING ISO/IEC 17065 & ETSI EN 319 403 AS THE CAB ACCREDITATION FRAMEWORK FOR TSP/TS ASSESSMENTS

The European cooperation for Accreditation (EA) promoted accreditation scheme, based on [ISO/IEC 17065], requires CABs to be certification bodies, and not simply inspection bodies or laboratories as CABs are required to certify the conformity of QTSPs/QTSs against the applicable requirements of the eIDAS Regulation.

The EA justified the choice of [ISO/IEC 17065] as a basis for accreditation of CABs for evaluating their competence in assessing TSP/TS as follows:

> *EA members unanimously selected ISO/IEC 17065 as the best option as basis for the accreditation of CABs in the context of conformity assessments of TSPs and trust services they provide, and in particular assessment of QTSPs/QTSs. EA experience is that ISO/IEC 17020 is not considered appropriate to assessment of conformance of requirements for the management system of the TSP, and it is considered that a review of the security management system of the TSP constitutes an important part of a TSP audit.*
>
> *Also, ISO/IEC 17020 does not impose a continued assessment by following deviations of the use of certification brands. Inspection processes tend to review the status of the items being inspected at a point in time whereas the requirements for a TSP need a more long term, continuous assessment as provided by a certification scheme. The issue of certification includes requirements for regular surveillance activities as well as specific requirements for ongoing quality and service improvement.*
>
> *On their own ISO/IEC 27006 and 17021 are not considered sufficient to cover assessment of specific service requirements. However, ISO 17065 was specifically designed to be extended to incorporate requirements from 17021, but the opposite is not true as ISO/IEC 17065 requirements do not fit well into ISO/IEC 17021.*
>
> *The industry requirement for public trust services, such as reflected in the CA/Browser Forum guidelines and in other national schemes for non-qualified trust services, strongly supports a clear indication of the technical compliance to good practice in industry. The aim of the ETSI EN 319 403 conformity assessment is also to allow an assessment of conformance to industry good practices as well as that the technical requirements of the Regulation are met. ETSI/CEN consider that any scheme which falls short of assessment against industry good practice will bring the acceptability of qualified trust services into question.*

There is no inconsistency between a certification by an accredited CAB and the SB having the final decision on whether or not the (Q)TSP/(Q)TS meets the eIDAS requirements. Art.3(18), referring to Regulation (EC) N°765/2008, makes it possible for the CAB to be a certification body, or an inspection body, or a laboratory, with the requirement that the CAB must be accredited for its competences to assess QTSP/QTS against all requirements of eIDAS. It is worth emphasising that the final decision is in the hands of the SB. The latter may rely upon the information provided by the (Q)TSP and in particular the CAR, but it is equally entitled to request further information and it may take duly justified decision (e.g. applying good principle of administration and principle of proportionality) that goes against the conformity assessment report.

It is worth stressing as well that the annual surveillance audit, which may be a requirement coming from the accreditation/certification scheme under which CAB is accredited and (Q)TSP/(Q)TS are audited (e.g. §7.9 of [ISO/IEC 17065] and [EN 319 403]), is not a requirement from the eIDAS Regulation. Nor is the requirement for a continuous assessment by the CAB. Those continued assessments and annual surveillance audits do not substitute ex-post supervisory activities of supervisory bodies.

XX-00-00-000-XX-X

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000