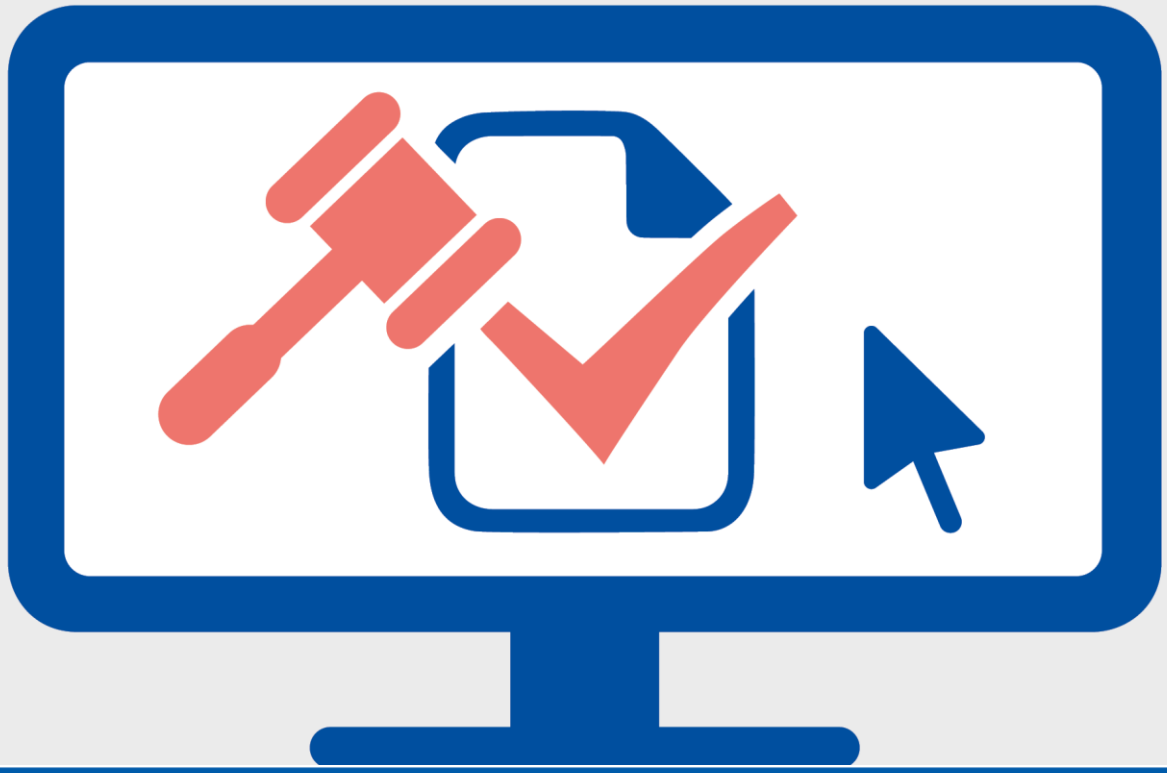
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



Recommendations for technical implementation of the eIDAS Regulation

Towards a harmonised Conformity Assessment Scheme for QTSP/QTS

DECEMBER 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.

CONTRIBUTORS

Olivier Delos (SEALED), Erik Van Zuuren (TrustCore), Hans Graux (Time.Lex), Olivier Barette (Nowina).

EDITORS

Evgenia Nikolouzou (ENISA), Slawomir Gorniak (ENISA), Dorin Bugneac (ENISA), Ioannis Agrafiotis (ENISA)

ACKNOWLEDGEMENTS

Special thanks go to various stakeholders in Europe who provided their response to the survey and/or were interviewed for the purpose of this report.

LEGAL NOTICE

COPYRIGHT NOTICE

TABLE OF CONTENTS

EXECUTIVE SUMMARY 6

1. INTRODUCTION 8

1.1 SETTING THE SCENE 8

1.2 THE NEED FOR A HARMONISED eIDAS QTSP/QTS CERTIFICATION SCHEME 10

1.3 PURPOSE OF THIS REPORT 12

2. STAKEHOLDERS' INPUTS 13

2.1 INTRODUCTION 13

2.2 THE VIEWPOINT OF SUPERVISORY BODIES 13

2.2.1 Foreword 13
2.2.2 On the EA recommended accreditation scheme 13
2.2.3 (Multipurpose) Certification scheme 14
2.2.4 Composite certification approach 15
2.2.5 Nationally defined schemes – Private schemes 16
2.2.6 Ownership and maintenance of harmonised certification scheme 16
2.2.7 Legal instruments 16

2.3 THE VIEWPOINT OF NATIONAL ACCREDITATION BODIES 17

2.3.1 EA inputs 17

2.4 THE VIEWPOINT OF CONFORMITY ASSESSMENT BODIES 19

2.4.1 Foreword 19
2.4.2 Being accredited as a CAB for eIDAS conformity assessments 19
2.4.3 eIDAS CABs are certification bodies 20
2.4.4 Cooperation - competition 20
2.4.5 Composite audits 21
2.4.6 Multipurpose audits 21
2.4.7 National specificities 21
2.4.8 Other aspects 21

2.5 THE VIEWPOINT OF OTHER STAKEHOLDERS 22

2.5.1 Browser Vendors 22
2.5.2 Adobe 25

3. ANALYSIS OF THE AVAILABLE LEGAL FRAMEWORKS 27

3.1 INTRODUCTION 27

3.2 eIDAS SECONDARY LEGISLATION 27

3.3 CYBERSECURITY ACT 30

3.4 eIDAS revision or amendment 32

4. GAP ANALYSIS – TOWARD A HARMONISED SCHEME 33

4.1 GENERAL PRINCIPLES 33

4.1.1 eIDAS Regulation driven 33
4.1.2 In-depth list of controls and control objectives 33
4.1.3 Technological neutrality – QTSP freedom of implementation 33
4.1.4 National specificities 34
4.1.5 Scheme owner & maintenance 34

4.2 MULTIPURPOSE AUDITS 34

4.3 COMPOSITE AUDITS IN THE CONTEXT OF eIDAS REGULATION 35

4.4 INTERNATIONAL ASPECTS 35

4.5 ISO/IEC 17067 35

4.6 LEGAL INSTRUMENT 35

5. RECOMMENDATIONS 36

5.1 OVERVIEW 36

5.2 ACTIONS REGARDING LEGAL INSTRUMENTS TOWARDS AN EU HARMONISED EIDAS CAS 36

5.3 ACTIONS REGARDING THE DESIGN OF EU HARMONISED QTSP/QTS CAS 38

5.4 CAS OWNER(S) 39

5.5 "QUICK WINS" 39

6. BIBLIOGRAPHY/REFERENCES 41

6.1 REFERENCES 41

6.2 BIBLIOGRAPHY 42

6.2.1 Applicable legislations 42
6.2.2 ETSI standards applicable to (Q)TSP/(Q)TSs 43

ABBREVIATIONS

AATL	Adobe Approved Trust List
BV	Browser Vendor
CA	Certification Authority
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CAS	Conformity Assessment Scheme
CEN	Centre Européen de Normalisation
CID	Commission Implementing Decision
CIR	Commission Implementing Regulation
DV	Domain Validated
EA	European cooperation for Accreditation
EC	European Commission
ECCG	European Cybersecurity Certification Group
EEA	European Economic Area
eID	electronic Identification
EN	European Standard
eRDS	electronic Registered Delivery Service
ESO	European Standards Organisation
ETSI	European Telecommunications Standards Institute
ETSI TS	ETSI Technical Specifications
EU	European Union
EV	Extended Validation
GDPR	General Data Protection Regulation
IAF	International Accreditation Forum
ICT	Information and Communications Technology
ISMS	Information Security Management System
ISO	International Organization for Standardization
MS	Member State
NAB	National Accreditation Body
OV	Organization Validated
PIMS	Privacy Information Management System
PKI	Public Key Infrastructure
QERDS	Qualified Electronic Registered Delivery Service
QESeal	Qualified Electronic Seal
QESig	Qualified Electronic Signature
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
QTST	Qualified Time Stamp Token
QWAC	Qualified Website Authentication Certificate
SB	Supervisory Body
SME	Small and Medium-sized Enterprise
TL	Trusted List
TLSO	Trusted List Scheme Operator
TS	Trust Service
TSP	Trust Service Provider
TSP/TS	Trust Service Provider and the Trust Service it provides

EXECUTIVE SUMMARY

The context - trust services and the European legal and standardisation framework for accreditation and conformity assessment

In the European Union, Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market [eIDAS, 2014] (hereinafter the eIDAS Regulation) introduced specific legal provisions in relation to trust services in general, and in relation to so-called qualified trust services in particular. Qualified trust service providers (QTSPs) and the qualified trust services (QTSs) they provide are bound by more stringent responsibilities, including in relation to quality and supervision.

As a prerequisite to entering the market and providing QTS, a prospective QTSP/QTS must first be audited by an eIDAS accredited conformity assessment body (CAB) to confirm, through a conformity assessment (audit) report (a CAR) that the QTSP and the QTS it provides meet the requirements of the eIDAS Regulation. Once the CAR has been created, the prospective QTSP must provide notice of its intention to provide QTS to its competent national supervisory body (SB). The SB will verify the conformance of the prospective QTSP/QTS to the eIDAS Regulation based on the submitted CAR and will grant or decline a qualified status.

The eIDAS Regulation however does not specify any particular accreditation scheme or any conformity assessment (or certification) scheme against which a CAB must be accredited. Instead, the eIDAS Regulation requires the CAB to be accredited in the framework of Regulation (EC) No 765/2008 [Reg.765, 2008], which is the generic European regulation in relation to accreditation. It furthermore requires that the conformity assessment scheme (CAS) used by the CAB is eIDAS specific.

Currently, 30 eIDAS CABs are accredited to perform conformity assessments in 11 EU Member States (MS), based on an accreditation scheme, which is recommended by the European cooperation for Accreditation (EA). The EA is the body recognised under Regulation (EC) No 765/2008 to manage a peer evaluation system across national accreditation bodies (NABs) from the EU Member States and other European countries. However, this scheme is not mandatory under the eIDAS Regulation, and EU MS may therefore elect to choose another scheme, provided that it can be shown to satisfy the eIDAS requirements. The scheme chosen requires eIDAS CABs to be certification bodies meeting the requirements of ISO/IEC 17065 supplemented by EN 319 403, with the eIDAS Regulation itself being the normative document against which the conformance of QTSP/QTS needs to be evaluated. The competence of the CAB to conduct such evaluations needs to be accredited by its NAB.

The challenge – variations in practice and the need for better harmonisation

A specific feature of the eIDAS accreditation scheme recommended by the EA, and intrinsically of the eIDAS Regulation as the normative document, is that the requirements against which the QTSP/QTS must be certified are technology neutral legal requirements, expressed in terms of functional objectives. Furthermore, no standard may be mandatorily imposed upon the QTSP for providing QTS in conformance with the Regulation in order not to negatively impact innovation and/or harm competition.

In addition, no eIDAS secondary legislation has been adopted to date to reference any standard that would create a legal presumption of compliance with any requirement of the eIDAS Regulation for the QTSP. As a result, there is significant margin of interpretation and for policy choices in creating, interpreting and applying accreditation and certification approaches.

The difference in approach and in assessment effort for accreditation of CABs and for the certification of QTSP/QTS is reported by a vast majority of stakeholders (including EA) as hindering the mutual recognition of accredited certification of electronic trust services.

The present report aims to propose ways in which the eIDAS assessment regime can be strengthened based on the current regime of the eIDAS Regulation, the stakeholders' concerns and the legitimate need to move towards a more harmonised approach with regards to the assessment by CABs of the conformity of QTSP/QTSs with the requirements of that Regulation. It focuses in particular on actions towards a harmonised conformity assessment scheme for QTSP/QTS.

The solution – potential roads forward

This report lists the following recommendations in moving towards a harmonised CAS for QTSP/QTS:

- **Actions regarding legal instrument(s)**. Formalisation of the CAS by the European Commission as an official scheme with legal recognition across EU via legal document(s).
- **Actions regarding the design of the harmonised CAS**. The design of a harmonised CAS by ENISA and the European Commission (under the Cybersecurity Act) or by the European Commission (under the eIDAS Regulation) can be based on ISO/IEC 17065, EN 319 403-1 and TS 119 403-3 "Additional req. for CABs assessing EU QTSPs", designed in accordance with ISO/IEC 17067 "Fundamentals of product certification and guidelines for product certification schemes".
- **Actions regarding continuous improvement of CAS**: Define process and involved actors for a harmonised CAS, governed by a scheme management authority (i.e. scheme owner) together with EU-wide representative working group, under a defined review method.
- **Quick wins.** EA, ETSI, and CABs actions could be implemented by each of them individually in the short term. Examples constitute the update of EN 319 403 and consequently TS 119 403-3, the update of EA-recommendations to refer to TS 119 403-3, and the non-issuance of certificates of conformity with identified pending non-conformities.

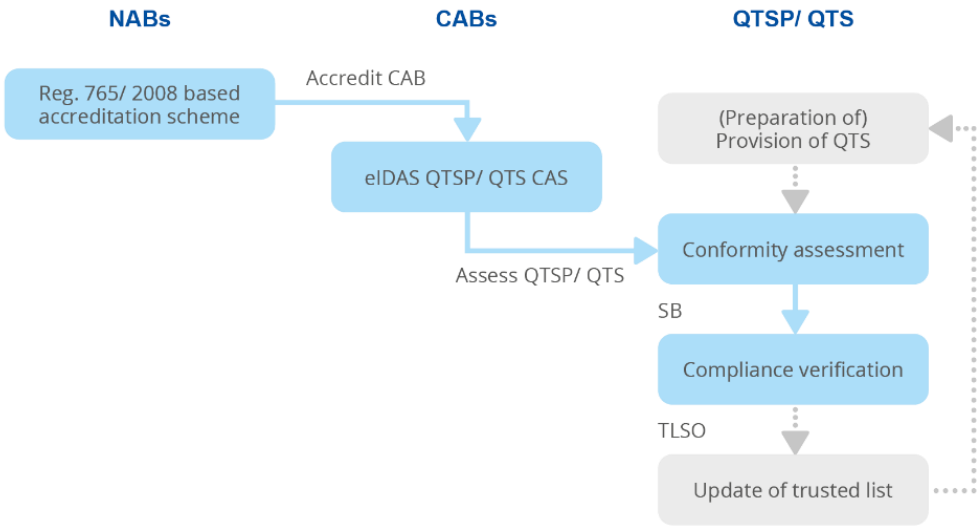
1. INTRODUCTION

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), 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 qualified status that allows providing QTSs, trust service providers (TSPs) and the QTSs they plan to make available must first demonstrate that they meet the requirements of the Regulation. This implies that TSPs and the QTSs at hand need to undergo a specific process and receive a 'green light' 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.

Figure 1. eIDAS QTSP/QTS compliance assessment and verification process



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 they meet the requirements of the eIDAS Regulation.

As the next step of the process, the prospective QTSP notifies its intention to provide QTS to its competent national supervisory body (SB) together with the positive CAR resulting from such an assessment. Considering such CAR, the SB will verify the conformance of the prospective QTSP/QTS with the eIDAS Regulation and will decide to whether or not to grant, 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. Instead, the eIDAS Regulation requires the CAB to be accredited:

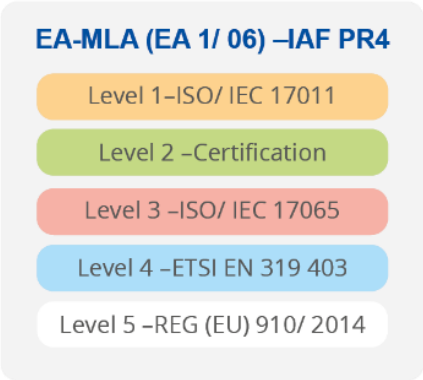
- In the framework of Regulation (EC) No 765/2008 [Reg.765, 2008]
- For the execution of a conformity assessment scheme that is eIDAS specific, i.e. confirming that, for a specific type of QTSP/QTS, a QTSP/QTS is meeting the applicable requirements of the eIDAS Regulation.

The European cooperation for Accreditation[1] (EA) is the body recognised under Regulation (EC) No 765/2008 to manage a peer evaluation system across national accreditation bodies (NABs) from the EU Member States and other European countries. EA has adopted the recommendation[2] to use an eIDAS accreditation scheme based on the [ISO/IEC 17065] accreditation framework, supplemented by [ETSI EN 319 403], as one possible route for CABs to assess conformity with relevant requirements of the eIDAS Regulation.

The eIDAS accreditation scheme recommended by the EA requires:

- The accreditation of the CAB is based on the [ISO/IEC 17065] framework.
- The [ISO/IEC 17065] accreditation framework of the CAB to be supplemented by [ETSI EN 319 403], which specifies additional dedicated requirements for CABs carrying out the certification of TSP/TS, towards defined criteria against which they claim conformance (those criteria being identified as the “Normative Document”).
- The accreditation of the CAB to confirm the skills and competence of the CAB to conduct conformity assessments of QTSP/QTS against the requirements of the eIDAS Regulation. Indeed, the scheme defines the Regulation as the Normative Document laying down criteria/requirements against which the QTSP/QTS conformance is to be assessed.

Figure 2: eIDAS accreditation scheme recommended by EA



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 general policy preference for technical neutrality. The Normative

[1] http://www.european-accreditation.org/
[2] 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 specify 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 they and the QTS provided meet the requirements of the eIDAS Regulation.

Finally, no eIDAS secondary legislation has been adopted to date to reference any standard that would create a legal presumption of compliance with any requirement of the eIDAS Regulation for the QTSP that choose to adhere to that standard or for the QTS it provides. However, even if such secondary legislation would have been adopted, compliance to such standards would still remain voluntary for QTSPs: their use remains optional.

1.2 THE NEED FOR A HARMONISED eIDAS QTSP/QTS CERTIFICATION SCHEME

The eIDAS accreditation approach that is recommended by the EA has been widely adopted by the European NABs (national accreditation bodies) that have accredited CABs in the context of the eIDAS Regulation. However, based on the situation described above and the legal and policy choices made by the European legislator, there is still significant diversity regarding the conformity assessment (certification) schemes used by those CABs in practice. This diversity results from the current accreditation framework that de facto requires CABs to define their own conformity assessment scheme.

There is no obligation for NABs or competent national supervisory bodies to provide guidance to CABs for designing an appropriate eIDAS conformity assessment scheme. It seems that very few NAB actually mandate CABs they accredit to go through a specific, [ISO/IEC 17067] based, process to define such an eIDAS conformity assessment scheme. Amongst the few other NABs and/or supervisory bodies, that are providing guidance on the list of controls and control objectives that should be used to assess QTSP/QTSs conformance to eIDAS, most of them are leveraging on ETSI standards[3], *as is* or by profiling them.

Despite the fact that most of the certification schemes defined by CABs (with or without guidance from competent authorities) are in whole or in part based on ETSI standards, when such standards are available, there is no visible coordination and no enforcement of a single scheme at EU level.

The quality of those standards, their adequacy for use by QTSP/QTSs to meet the requirements of the eIDAS Regulation and hence their eligibility for being referenced to meet the requirements are still to be formally assessed and demonstrated.

Most CABs do not make conformity assessment scheme documents they use in practice publicly available. As a result, relying parties are hampered in their legitimate quest for trust and accountability, and cannot obtain a reasonable confidence that QTSP/QTSs meet the requirements of the eIDAS Regulation.

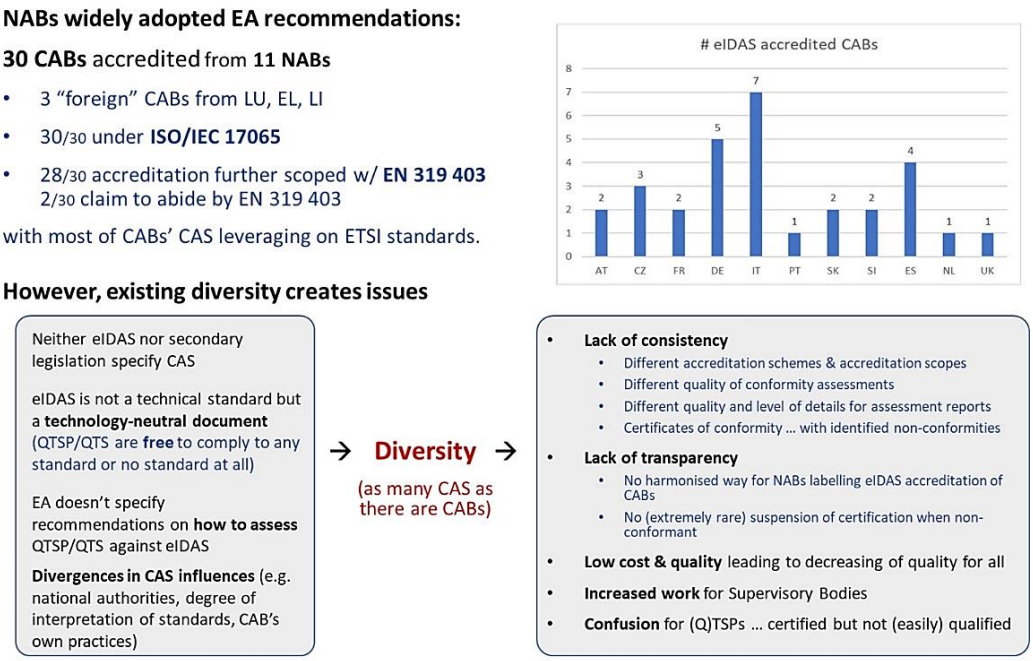
Furthermore, despite the peer review mechanism imposed at the level of NABs by Regulation (EC) 765/2008, there is little or no assurance on the quality of the currently accredited CAB certification schemes to enable the CAB to confirm effectively that assessed QTSP/QTSs meet

[3] See section 6.2.2.

the eIDAS requirements. QTSPs may use a CAB located anywhere in the EU and accredited by a NAB from a different country than the one in which the QTSP is established. Supervisory bodies experienced that CARs from different eIDAS accredited CABs may differ significantly not only a difference in the formal approach used by such CABs, but also and more importantly a diversity in terms of quality and adequacy of their assessments against the eIDAS Regulation.

Concerning non-EU countries, it became clear that the IAF MLA driven accreditation scheme based on [ISO/IEC 17065] (potentially supplemented by [ETSI EN 319 403]) is a candidate for such countries to base their national QTSP/QTS certification scheme on, particularly for other QTS than issuing qualified certificates[4]. Moreover, it is possible and usual for such 3rd countries to expand and finalise the ETSI EN 319 403-based scheme by the establishment of a harmonised, specific and complete certification scheme. This scheme will lay down to a sufficient level of technical details, the exact set of controls and control objectives that the CAB will have to use to conduct a conformity assessment of a QTSP/QTS against more generic legal provisions. This may be facilitated by the fact that national legislations may reference standards as binding normative documents (contrary to the eIDAS Regulation). Moreover, 3rd countries point out that the EA recommended scheme is incomplete and falls short of a harmonised eIDAS certification scheme. This jeopardizes a mutual recognition of EU QTSP/QTSs, simply because the diversity in conducting the audits of QTSP/QTS over EU might not guarantee an acceptable level of reliability compared to the 3rd country applicable scheme.

Figure 3: Existing diversity in CAS creates issues



One of the prime purposes of the eIDAS Regulation is to establish an EU wide recognition of the legal effects attributed to qualified trust services and their outputs (e.g. "*A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States*", Art.25(3)). To this

[4] The scheme based on ISO/IEC 17065 and supplemented by ETSI EN 319 403 is applicable to any type of TSP/TS for being assessed to any type of standard, technical specification or regulation. It is completely independent of the eIDAS Regulation. The EA recommended eIDAS scheme is adding to this generic scheme the eIDAS Regulation as the normative documents against which the QTSP/QTS need to be assessed conformant. Any non-EU 3rd country may act similarly by adding its own regulatory or technical specifications as normative criteria against which national TSP/TS need to be assessed conformant.

extent, it is critical for the requirements against which QTSP/QTSs are assessed to be comprehensive, consistently applied and sufficiently detailed to reduce the scope for variances in the assurance provided in the trustworthiness across different QTSP/QTSs. The lack of a harmonised scheme concerning the accreditation of CABs and the conformity assessment (certification) of QTSP/QTSs may:

- Introduce risks due to inconsistent standards and controls being applied.
- Diminish potentially the overall confidence in the eIDAS regulated QTSs.
- Impact negatively the trustworthiness and acceptability of these QTSs not only in the EU internal market, but also when interoperability with non-EU countries or international organisations is considered, and when recognition of QTSs in widely deployed applications or browsers is targeted.

Therefore, a key issue to address is the move toward harmonisation of conformity assessment of QTSP/QTSs, and of related conformity assessment schemes in particular.

1.3 PURPOSE OF THIS REPORT

The present report aims to propose ways in which the eIDAS assessment regime can be strengthened based on the current regime of the eIDAS Regulation, stakeholders' concerns and legitimate needs to move towards a more harmonised approach for the assessment of the conformity of QTSP/QTSs with the requirements of that Regulation,. It focusses in particular on actions towards a harmonised conformity assessment scheme for QTSP/QTS.

- **Section 2** describes inputs collected from relevant stakeholders on the assessment of QTSP/QTSs in the context of eIDAS.
- **Section 3** analyses the available legal framework and instruments to support actions towards a harmonised conformity assessment scheme for QTSP/QTS.
- **Section 4** analyses the gaps towards such a harmonised scheme.
- **Section 5** proposes concrete actions towards such a harmonised eIDAS QTSP/QTS conformity assessment scheme.

2. STAKEHOLDERS' INPUTS

2.1 INTRODUCTION

This part addresses inputs concerning the assessment of QTSP/QTSs in the context of eIDAS as collected from relevant stakeholders, including (Supervisory Bodies) SBs, NABs, CABs, QTSPs, and other stakeholders such as browser or application vendors.

2.2 THE VIEWPOINT OF SUPERVISORY BODIES

SB / EU MS

Urging for harmonised CAS, with:

- Clarifying CAR details and contents
- Hermonisation in NABs delivering accreditation
- Handling multipurpose audits (need for clear eIDAS compliance statement)
- Clarifying composite certification approach
- Allowing for national specificities
- Clear ownership and maintenance
- Legal instrument support

2.2.1 Foreword

The study team received inputs from 7 SBs out of the 31 SBs. All responsive SBs agree on the need for harmonisation of QTSP/QTSs conformity assessment (or certification) schemes used by eIDAS accredited CABs. Their main inputs may be summarised as follows.

2.2.2 On the EA recommended accreditation scheme

While the EA recommended scheme based on ISO/IEC 17065 in combination with [ETSI EN 319 403] is accepted to be the correct way in going forward towards harmonising the eIDAS CAB accreditation and QTSP/QTS certification schemes at the EU level, the need for a number of improvements have been identified by most of the responsive Member States:

a) **Clarification on details and content of audit reports and conformity declarations**:

- It appears that at times, NABs might not be fully aware of the importance and the purpose of the CAR in the eIDAS framework. The fact that the CAR must be sent to the SB (where in general use of the [ISO/IEC 17065] for product or service certification, the assessment report is for the certification holder only) and the fact that the SB relies heavily on the content and the completeness of the CAR are new to most of the actors involved. In the context of its recommended eIDAS scheme, the EA should consider clarifying the importance of the CAR as essential input for the decision of the SB and that no barrier should be placed to its dissemination to the competent SB.
- The recent publication of [ETSI TS 119 403-3] is welcomed as it specifies additional requirements for CABs assessing eIDAS QTSP/QTSs focusing on the structure and content of eIDAS CAR. The CAR is an essential element for the SB to base its

verification of the compliance of the assessed QTSP/QTS with the applicable eIDAS requirements and, if granting a qualified status, to express in a correct way the corresponding qualification decision in the Trusted List. Responsive SBs experience significant differences in the scope and quality of the received CARs (e.g. minimum content not always present, length and level of details highly varied and sometimes insufficient, occurrences of significant errors or omissions, and sometimes not sufficiently elaborated evaluation reports). EA should consider extending its currently recommended eIDAS scheme with this [ETSI TS 119 403-3] standard.

- The next update of the current version of [ETSI EN 319 403] (expected to be published under the reference EN 319 403-1) should also be considered for updating the current EA recommended scheme. Particularly, EN 319 403-1 should include important corrections regarding the management of non-conformities in the process of issuing certification declarations (attestations). Reporting requirements and the way for handling non-conformities and/or other non-critical issues (e.g. area of improvements) must be part of the accreditation scheme.
- Further guidance should be provided on the minimum audit time and effort for completion of the full assessment and surveillance assessment respectively. The quality and the credibility of an assessment are based primarily5 on two factors: (1) the audit time for completion of full assessment and (2) the level of expert-knowledge of the auditor/audit team. Taking into consideration that these factors are also the main cost-drivers, the risk exists that in a competitive market, the quality and credibility of the assessment becomes subordinate to the price of the assessment.

b) **Further harmonization between the different NABs delivering accreditation**:

- The way NABs are wording the scope of the accreditation of CABs in the context of eIDAS is far from being harmonised. The feeling exists that the NABs are not fully aware of the nine types of QTSP/QTSs specified in the eIDAS Regulation and that the corresponding certification scheme(s) must target the corresponding requirements (or articles) of the eIDAS Regulation.
- The way CAB accreditation certificates are maintained by NABs is also not harmonised and does not seem to ensure the provision of historical information regarding the grant of the accreditation on a per QTSP/QTS type basis.
- When the EA recommended eIDAS accreditation scheme is not used or not entirely used, it is not easy to identify whether the alternative scheme has been determined equivalent and under which basis. From a supervisory point of view, responsive SBs believe it is highly desirable to have [ETSI EN 319 403] being part of the requirements.

2.2.3 (Multipurpose) Certification scheme

Most of the eIDAS certification schemes used by CABs, that the reporting SBs have experienced, are based on relevant ETSI standards. Especially for certificate-based trust services, many of these schemes are multi-purpose certification schemes. They include requirements from the CA/Browser Forum (Baseline [BRG] and EV [EVG]) as well as local/national requirements.

Already in the context of a single-purpose (eIDAS) certification scheme, it is experienced that it can be very difficult to identify which certification scheme, and hence which requirements, criteria, checks and/or tests, have been used by the CAB to conduct the assessment and the extent to which they have been used. Even if the certification scheme is referred to in the CAR,

[5] Other factors such as for example efficient audit procedures and used tools for automation of audits should be taken into account to define the quality and the credibility of an assessment.

it is not always clear which concrete measures are put in place by the QTSP and assessed by the CAB before delivering a conformity attestation.

As the eIDAS requirements are expressed in terms of functional objectives, there is a need for more concrete criteria (technical and organizational) for allowing proper assessment. The use of the QTSP/QTS relevant requirements in the appropriate ETSI and CEN standards are recommended as a basis for designing QTSP/QTSs harmonised certification schemes. It is believed that this can be done in a way not hindering the technology neutral approach of the eIDAS Regulation and leaving QTSP freedom of choosing the technical standards of choice.

Reporting requirements and the way for handling non-conformities and/or other non-critical issues (e.g. area of improvements) must be part of the certification scheme if not explicitly handled in the accreditation scheme.

In general, and in particular for multi-purpose certification schemes, it is advised to make use of as many distinct declarations (attestations) of conformity as there are identified purposes.

There is an expectation that a good policy choice to develop eIDAS certification schemes could stem from the recommendations of [ISO/IEC 17067].

2.2.4 Composite certification approach

Splitting operations and responsibilities regarding the provision of a trust service into various component services used between the TSP itself and 3rd parties is common practice among customers. For example, a TSP issuing electronic certificates may limit its effective operation to bear the overall and final liability on the trust service it provides on its contracted customers, while outsourcing completely the operation of all component services (including registration and enrolment of customers (RA), certificate validity status information services, repository services, PKI factory services, etc).

It is also a trend for such 3rd parties to specialize in the provision of (Q)TS component services and to offer their expertise to many different TSPs.

Responsive Member States believe that a harmonised certification model to allow different (Q)TS components to be assessed independently, with the aim for an appropriate aggregation to support the assessment of the overall (Q)TS, without having to repeat a full assessment of all components again. This would allow the CAB to take into consideration earlier audit reports/certification decisions when performing the assessment of a QTSP/QTS. Rules for accepting existing and underlying certification must nevertheless be established, e.g.:

- Valid certificate not older than “x” (e.g.12) months;
- Components may only be used as long as they maintain a valid certification of an accredited CAB;
- Usage of the component must be discontinued once the components certification expires or is withdrawn;
- The way earlier assessments and certifications are taken into account must be described in the certification scheme and documented in the assessment report;
- Verifying how an earlier “generic” certification of a component service applies in the case of a specific instantiation (or use) of that certified component service in the context of the assessment of the overall QTS. The integration of the component service into the assessed QTS must be examined: in particular the interface(s) through which the component is integrated must be considered.

The certification of “Remote QSCD operation and management”[6], of “(Q)TS managed service components”, of “registration authorities” and in particular the certification of "remote identification procedures" foreseen in Art.24(1) of eIDAS are amongst the first composite certification schemes needed.

2.2.5 Nationally defined schemes – Private schemes

In several Member States, a scheme for the accreditation of CABs and for the certification of QTSP/QTSs has been defined and managed either by a national competent authority (usually a SB, or a NAB in collaboration with a SB) or by a private entity.

While most, when not all, of these schemes are built upon the same set of European standards (e.g. ETSI x19 xxx and CEN 419 xxx series) and international standards, they include variances (sometimes significant) in the standard references or profiling. This may induce different/unequal treatment of CAB between Member States and force CABs willing to operate in different Member States to consider as many different interpretations as there are nationally-defined schemes, despite the “certified once, recognised everywhere” International Accreditation Forum IAF principle to which European NABs and Regulation (EU) 765/2008 subscribe.

2.2.6 Ownership and maintenance of harmonised certification scheme

As a lesson learned from experience with such nationally-defined or private schemes, responsive EU MS believe it is vital to have an active scheme owner that maintains the scheme and provides documented guidance on how to apply it. TSPs tend to innovate, technology is in constant evolution, and so are the risks and challenges around trust services. This means CABs using the certification scheme will encounter new situations and will require guidance on how to apply the scheme in consequence. The work of harmonising an EU-wide eIDAS certification scheme would be incomplete if it did not address appropriately how the scheme can be maintained and how harmonised guidance can be provided to its users in the future.

2.2.7 Legal instruments

Responsive SBs believe guidance on the accreditation scheme for CABs should be settled in EU legislation. They stress the current absence of implementing acts, in particular concerning CAB accreditation and rules on auditing and audit reporting (i.e. Art.20. 4 of eIDAS) but also concerning QTSP/QTS requirements. Some of those SBs would prefer to see CAB related standards become mandatory.

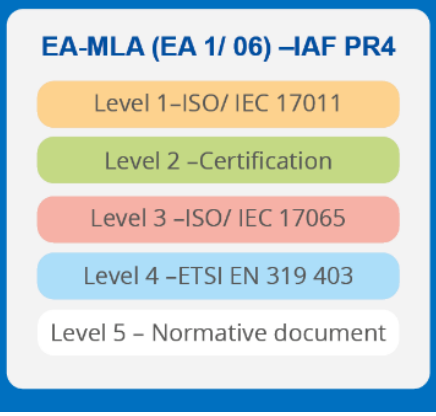
[6] Note the ILNAS, the LU SB, provide “*requirements for qualified trust service providers issuing qualified certificates for electronic signature or for electronic seal in the case where the electronic signature creation data resp. electronic seal creation data are managed by the qualified trust service provider on behalf of the signatory resp. creator of seal*”. CAB has to check whether those requirements are fulfilled.
https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/confiance-numerique/surveillance-psc/procedures/ilnas-pscq-pr001-supervision-en/ilnas-pscq-pr001-supervision-en.pdf

2.3 THE VIEWPOINT OF NATIONAL ACCREDITATION BODIES

SB / EU MS

Agreeing on benefits from harmonised CAS

- EA has no mandate/authority to define CAS or to amend standards to refine scheme
- Cureent EA recommended scheme may be exended to CAR specification (e.g. TS 119 403-3)
- Current EA recommeneded scheme might be promoted at IAF level



2.3.1 EA inputs

EA has recommended [ETSI EN 319 403], supplementing the [ISO/IEC 17065] accreditation framework as a suitable scheme for the accreditation of CABs assessing QTSP/QTSs against the eIDAS Regulation as normative document. It is a preferred option, not a compulsory one. Each NAB may adopt it for use or use another scheme, provided the framework they use is equivalent to [ETSI EN 319 403] (at least, if they are EA members). E.g. UKAS uses two schemes, namely [ETSI EN 319 403] and tScheme[7].

The EA may not impose its recommended ISO/IEC17065+EN319403+eIDAS scheme; it may simply try to convince competent authorities of the merits when using it. The eIDAS Regulation does not give any mandate to the EA for doing so and is not specific for what regards accreditation[8]. The EA believes it would be up to the EC, or the legislative body, to make a decision on the (mandatory) use of [ETSI 319 403].

> **Note 1:** Ideally, [ETSI TS 119 403-3] should better be used as the basis for the EA recommended eIDAS scheme, supplementing [ETSI EN 319 403], or even better supplementing the next updated version of that EN to be published as ETSI EN 319 403-1.

> **Note 2:** The adoption of an implementing Act pursuant to Art.20.4 of eIDAS would allow referring to [ETSI 319 403] or better [ETSI TS 119 403-3] further supplementing its updated version EN 319 403-1. However, it is unlikely that these standards will be made mandatory via this legal instrument to NAB for the accreditation of CABs under eIDAS (and for CABs to carry out their conformity assessment of the qualified trust

[7] https://www.tscheme.org/
[8] Basically, it is the same issue as the one that applies for TSP's audit criteria but at the level of the CAB's accreditation framework.

service providers). The current revision process of the eIDAS Regulation would also be an option for the amended Regulation to be more prescriptive on the standards for accrediting CABs, for the conformity assessment report and for the rules on conducting QTSP assessments. Another option would be the certification scheme adoption process foreseen in the EU Cybersecurity Act [CyberAct, 2019]. Section 3 in this report sets outfurther discussions on appropriate legal instruments.

The EA recognises that having one single accreditation/certification scheme would be beneficial and that this scheme should go as deep as to address the scoping against the applicable requirements of the eIDAS Regulation. At such a deeper level, EA noted that there is however no guidance at the EA level on scoping [ETSI EN 319 403] against the Regulation being the normative document. In other words, there is no EA guidance on detailing how to design an appropriate eIDAS certification scheme, i.e. on detailing which criteria to be used by CABs to evaluate and demonstrate QTSP/QTS conformance to eIDAS.

It should be stressed that EA and NABs do not have the authority to amend standards to further refine the accreditation scheme down to the level of CAB certification scheme. Another "authority" should take this under its responsibility (e.g. ESO, ENISA, EU MS, EU MS SBs, eIDAS EU MS Experts Group). There is a need for cooperation between the relevant "authorities" to define such schemes and probably as many schemes as there are types of QTSP/QTS defined in eIDAS. Such definitions may or should leverage on existing and potentially amended versions of relevant ETSI standards for QTSP/QTSs.

In collaboration with the study team, EA will conduct a survey amongst its members in preparation of one of the next EA Certification Committee meetings. After three years of implementation of the EA recommended eIDAS accreditation scheme, it would indeed be the time for identifying and analysing some return on experience and lessons learned. Based on the EA Certification Committee's decision on this topic, the EA Working Group - ICT and Data Security (WG ICTDS) could be solicited to propose ideas and/or concrete actions. At the date of finalising this report, the survey was not completed. However, preliminary feedback provided by the EA confirms the diversity of approaches used by EA members with regards to guidance or requirements on conformity assessment schemes (CASs), within a common generic framework based on ISO/IEC 17065 and ETSI EN 319 403. It also indicates that EA members that did not benefit from a nationally defined CAS experienced issues with CAR suitability to support sufficiently a SB's informed decision to grant a qualified status. Most of the responsive member urge for the establishment of an EU harmonised CAS. The difference in approach and in assessment effort for accreditation of CABs is reported by a member as hindering the mutual recognition of accredited certification of electronic trust services.

Concerning the extension of the accreditation scope (e.g. ISO/IEC 17065 + EN 319 403) to [ETSI TS 119 403-3], existing EA defined procedures can be used by NABs at the request of CABs. CABs may apply and ask their NAB to include TS 119 403-3 in the scope of their accreditation. National authorities (e.g. SBs) might also require the CABs to do so, e.g. to facilitate SBs' decision process for granting or confirming a qualified status to (Q)TSP/(Q)TSs.

Regarding the international aspects, i.e. the promotion of [ETSI EN 319 403]-based accreditation scheme at IAF level, EA may approach the IAF Technical Committee to enquire about the applicable and relevant process to promote [ETSI EN 319 403] (or [ETSI TS 119 403-3]) based accreditation scheme at the IAF level. However, such a process is likely to take quite a long time to reach concrete results. EA believes that an ideal option would be for [ETSI EN 319 403] (or [ETSI TS 119 403-3]) to become an ISO standard or to create a bridge standard between relevant ISO and ETSI standards.

2.4 THE VIEWPOINT OF CONFORMITY ASSESSMENT BODIES

CABS

Agreeing on benefits from harmonised CAS

- Providing for guidance in evaluating compliance with eIDAS
- Clarifying certification decision versus SB's decision to grant or not a qualified status
- Supporting set-up of cooperation working group betewwn CABs
- Handling composite and multipurpose audits
- Handling national specificities
- Innovation supportive
- Harmonising efforts and surveillance programms

2.4.1 Foreword

All 30 CABs informally reported by the EC[9] as accredited against the requirements of the eIDAS Regulation have been accredited under the [ISO/IEC 17065] framework. For two of them, the "scope of accreditation" provided by the corresponding NAB does not (clearly) indicate this framework being supplemented by [ETSI EN 319 403], however both CAB certification schemes claim to abide by this standard.

Amongst the currently 30 eIDAS accredited CABs, very few are publishing or providing upon request a copy of their accredited eIDAS conformity assessment (or certification) scheme. Making this information available on request is, however, an obligation for ISO/IEC 17065 accredited CABs, as per clause 4.6 of [ISO/IEC 17065].

Amongst the identified CASs used by the eIDAS accredited CABs, four main categories can be identified:

- CASs that are fully specified by national authorities (e.g. SBs in CZ, SK) and are mandatory for use by CABs nationally accredited under eIDAS;
- CASs that are fully established by national authorities (e.g. SB from FR), which are not mandatory for use by CABs accredited under eIDAS but may be used by them, providing a presumption of compliance to assessed QTSP/QTS when successfully audited against these CAS;
- CASs that are partially guided by specific requirements driven by national authorities (e.g. SBs and/or NABs like in BE, ES, IT, LU, MT, NL);
- CASs that are fully driven and defined by CABs without specific guidance from national authorities.

The next subsections summarise the input provided by the CABs to the study team.

2.4.2 Being accredited as a CAB for eIDAS conformity assessments

Being accredited as a CAB may represent both a significant investment and risk for newcomer bodies. For a market to be open and efficient, new players usually ask for certainty and clear rules

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

on how to be compliant, making sure in advance that their investment will result in their successful accreditation. The absence of clear rules, or at least of sufficient guidance, may represent an entry barrier and favour existing players, hampering the diversity of CABs.

In the absence of an EU-wide harmonised conformity assessment scheme or of guidance from national authorities (e.g. SBs), each CAB has to define its own scheme. New CABs are in search of guidance that they typically find in ETSI standards, ENISA guidelines, or nationally-defined schemes (e.g. [ANSSI, 2017], [NSA-CS], [DKPv2]). This significant upfront investment for a definition of a scheme may be thought unnecessary, as the resulting situation is that most of the certification schemes defined by CABs are in whole or in part based on the same ETSI standards. As the CAR needs to demonstrate meeting each applicable eIDAS requirement, the schemes are structured typically as a mapping for each of the eIDAS requirements for QTSP/QTS. These requirements are guided from controls (criteria) and control (criteria) objectives taken from these ETSI standards, supplemented for identified gaps by more generic standards such as ISO 27001, or other legal frameworks such as GDPR for data protection. Would a CAB aim to target a wider market than its homeland market, the variances between applicable nationally-defined schemes[10] may create additional burden to align the scheme of the CAB. Coordination / harmonization / centralization among CABs, NABs and SBs would greatly improve the process, and additionally lower the above-mentioned entry barrier.

It is worth noting that the ETSI standards aimed to support the implementation of the eIDAS Regulation were drafted first as standardized requirements for specific PKI-based implementations of QTSP/QTS. They provide less guidance or no guidance at all for the audit of "alternative", "innovative" or "creative" implementations of the eIDAS requirements. In these specific cases, the CAB may have to transpose its regular practices, checklists and controls. This ad hoc transposition usually occurs "on the spot" during the preparation phase between stage 1 and stage 2 of that audit. In addition, as the demonstration of skills and competence of the CAB during its accreditation by the NAB was performed most probably on an "ETSI-based standard case" and not against the Regulation, the quality of this particular conformity assessment might be at risk.

2.4.3 eIDAS CABs are certification bodies

As CABs accredited under [ISO/IEC 17065] are certification bodies, they issue a certificate in addition to the CAR resulting from their audit of a QTSP/QTS. The situation may be misleading as this certificate testifies that the assessed QTSP/QTS conforms to the applicable eIDAS requirements from the viewpoint of the CAB. Such a certificate of conformity is (as required by EN 319 403) published on the CAB's website as soon as the audit is successful, which will likely occur before the decision of the SB to grant a qualified status to the assessed QTSP/QTS. As the decision to grant such a qualified status is ultimately the responsibility of the competent SB, it may happen that the decision of the SB differs from the CAB's certification decision. This may create confusion for relying parties and should be addressed as much as possible in the harmonised certification scheme.

2.4.4 Cooperation - competition

The eIDAS Regulation does not regulate or address the cooperation between CABs. Most CABs are private companies, and in competition with each other in an open market. This may make a CAB cooperation working group difficult to setup as existing players may typically protect their long-invested expertise, as opposed to newcomers who will likely be in favour of sharing experiences.

[10] The variances pointed to here do not only address areas where the EU Member States are entitled to adopt national provisions (e.g. certificate suspension, Art.24(1).d alternative identification methods) but address those variances in interpreting the way common provisions from the eIDAS Regulation should be implemented by QTSP/QTS.

Nevertheless, the establishment of such a CAB cooperation-working group could facilitate harmonization of the application of conformity assessment approaches and criteria, particularly in a situation where each CAB designed its own scheme. Even in the case of a harmonised EU-wide certification scheme, equally accredited CABs may differently interpret and apply the conformity assessment criteria, resulting in hard to compare certifications of QTSP/QTSs. Some related ETSI standards help to partially mitigate these discrepancies, but not to an acceptable extent. Additionally, there is currently no 'legally resilient' link between eIDAS and the ETSI standards.

The set-up and functioning of such a CAB cooperation working group would only be efficient if every eIDAS accredited CAB, as well as CABs interested in becoming eIDAS accredited, could participate free of charge and on a voluntary basis[11], all having equal voice and vote.[12] It would be key as well that such a group shall tightly cooperate with SBs (e.g. FESA, EU MS eIDAS expert group members), ENISA and the European Standardisation Organisations.

2.4.5 Composite audits

With the growing number of specialised component service providers (e.g. CA factory, identification service provider under Article 24.1(d) of eIDAS, QTSP hosting a remote QSCD, service provider for eRDS), the harmonised certification scheme should take into account the handling of composite audits, where components of a QTS are audited separately by different CABs.

National frameworks exist for the recognition of such component audits by CABs in charge of the QTS audit, such as in Germany[13] or in The Netherlands under former Directive 1999/93/EC[14]. The recognition of such component audits at the European level should be included in the harmonised scheme, including the handling of possibly different validity periods for each of the resulting audit reports.

2.4.6 Multipurpose audits

The most common situations where multipurpose audits are required by (Q)TSPs to address their need or wish to be assessed as conformant to CA/Browser Forum requirements, and/or to specific ETSI standards.

2.4.7 National specificities

In practice, a CAB has to take into account the national specificities of the country of establishment of the QTSP (e.g. certificate suspension is forbidden in several EU countries, the existence of nationally-defined eIDAS certification schemes, or SB-specific requirements). This leads to the definition of a mainly common scheme with national variations. An EU-wide harmonised certification scheme should address this issue and resolve it.

2.4.8 Other aspects

The fact that most of the certification schemes defined by CABs are in whole or in part based on the same ETSI standards could be seen as hampering the technological neutrality of eIDAS. QTSPs may favour the lower risk “ETSI path” for implementing their QTS instead of a “creative” one where the demonstration of conformity to eIDAS would be more complex and the outcome of the eIDAS audit uncertain.

[11] Alternatively, membership could be automatic.
[12] Different initiatives have popped up recently like www.acab-c.com or the German working group of (German) recognized certification bodies (AGAB). Unfortunately, none of these initiatives managed to group a significant number of eIDAS accredited CABs and so far may not be considered as representative of the eIDAS CABs.
[13] Composite certification approach exists in Germany since 2007 for QTSP/QTS (or CSP at that time). It was part of the German assessment scheme for German eSignature Act (called Module-Confirmation).
[14] Composite assessment was covered by the TTP.nl scheme maintained by the iTrust foundation as a scheme operator, and actively used by all CABs operating in NL at that time.

In the absence of recognition of composite audit, a QTSP is forced (or at least highly constrained in its choice) to select the same CAB as the one having audited the component they use, for purely organisational and economic reasons. The risk that another CAB would challenge the outcome of the audit of the component is avoided, and the CAB may propose shorter audit time and lower budget because of the existing "partial audit". (Note: This is particularly the case if the component is located in another country and its audit would involve travels and associated costs).

Regarding the recurrence of audits, the carrying out of surveillance audits is typically at the discretion of the CAB, where the eIDAS Regulation only enforces 2-yearly audit of QTSP/QTSs. When imposed by the CAB or by a nationally-defined scheme or SB, the surveillance audit is typically performed on a yearly basis between two full audits. This may also be a topic for harmonisation.

The treatment of non-conformities is not harmonised and some CABs / SBs considered that QTS could be listed with pending (minor) non-conformities. This is also mainly due to a wrong approach in the current version of [ETSI EN 319 403], which should be corrected in the upcoming updated version, to be published as EN 319 403-1.

2.5 THE VIEWPOINT OF OTHER STAKEHOLDERS

BROWSER VENDORS

Supporting CAS harmonisation with more

- Transparency, consistency, accountability and enforcement mechanisms
- Clear aim and scope of audit reports
- Monitoring

However mutual recognition is not part of the BVs' trust framework

They do not envisage surrending their ability to enforce policies or requirements to CAs and their ability to exlude or distrust any non-conformant CA.

They plead for unkeyed QWACs attesting link between domanin name and its owner.

2.5.1 Browser Vendors

Discussions have been initiated between the European Commission and browsers and applications industry stakeholders for the recognition of eIDAS QTS in their widely deployed products and services.

Despite the highly visible and notorious integration of EU trusted lists-based validation of eIDAS qualified electronic signatures and seals in the Adobe Acrobat™ suites[15], those discussions have not led to significant progress in integrating QTS, qualified website authentication certificates (QWACs) in particular, in the widely deployed browsers. From the viewpoint of browser vendors (BVs), this is less a question of distrust (even if there are areas for

[15] https://acrobat.adobe.com/be/en/sign/capabilities/eidas.html

improvements) than a question of not delegating any trust decision regarding their trust frameworks or programs.

As a general approach, browser vendors claim to operate their own mature trust framework for entrusting (CA) certificates in their products and applications. In a similar way as EU MS SBs are acting towards QTSP/QTS, BVs act towards CA (TSP issuing certificates) verifying and deciding themselves on whether they are meeting

- CAs own policies as defined in their applicable CP/CPS,
- policies and requirements defined by the CA/Browser Forum, and
- additional requirements defined in their CA trust store program.

BVs ultimately own the trust decision for which CAs are included in their trust framework.

As part of this BV-driven verification and decision process, BVs require 3rd party audits to attest that the CA have complied with the above two first set of policies and requirements. All BVs recognise and "trust" both the WebTrust and ETSI audit schemes (the latter being commonly used to support the eIDAS framework as well). It is commonly stated by BVs that both audit tracks have areas of concern and potential improvement. However, as these audits are "only" one element amongst others supporting each decision on trusting a CA, trusting the audit scheme is not an absolute necessity. On top of these audits, BVs are conducting their own regular (risk) assessments to inform their trust decisions. They also support such decisions by active and transparent technical (PKI) monitoring.

When comparing the two types of trust frameworks, namely the one(s) established by BVs on one hand and the eIDAS framework on the other hand, it is important to stress that, contrary to the eIDAS framework, the BVs do not have and do not aim to implement mutual recognition. In the BVs' trust framework, there is no room for accepting trust decisions made by 3rd parties to lead (automatically) to trust decisions within the BV framework. In case of an Art.14 based mutual recognition between the EU and a 3rd country, the EU MS will not have to verify whether new or existing 3rd country trust services meet the eIDAS requirements. Verifications by the 3rd country, under the terms of the Art.14-based agreement will be automatically trusted by all the EU MS and the corresponding 3rd country verified trust services will be recognised as equivalent to QTS in the EU. This does not and is not likely to occur with BVs, who will base their CA trust decisions on the basis of their own verification of the conformance of each and every CA with their own requirements, irrespective whether they are otherwise qualified under eIDAS (or even already trusted by another BV). BVs do not rely on another entity's trust decision or delegate trust decision to any entity. They use other entities' decisions as input to better informed decisions, such as external audits which are part of BV's requirements. BVs may trust differently WebTrust and ETSI certification schemes, as well as auditors performing them. The overall BV's own decision process adjusts and corrects these differences, as the overarching goal is to evaluate all the available information against BV specific trust framework policies and requirements to ensure their users are secure.

It is worth noting that most of the BVs do not have a contractual relationship with CAs (TSPs). This means that those BVs have no legal recourse if a CA fails to meet their requirements. The relationship is based on whether or not the CA's root certificate is and remains to be included in BV's root store, based on the CA's continued compliance with BV's requirements. BVs authority rests in the ability to choose which CAs are members of their program. Taking that away greatly diminishes BVs' ability to influence good CA behaviour.

Regarding the ETSI audit track (which is also typically the basis for eIDAS conformity assessments), BVs identify opportunities for improvement falling into the categories of consistency, transparency, and enforcement.

The aim and scope of the audit reports must be very clear. Since no standards may be imposed to QTSPs issuing QWACs for being assessed compliant to eIDAS, being certified against eIDAS does not mean being certified compliant with any standard, even if used as benchmark criteria by auditors, unless the scope of certification makes it clear that, in addition to being eIDAS compliant, the QTSP/QTS are compliant to specific standard(s). The eIDAS requirements are intrinsically non-technical but functional and legal; the BVs' requirements are essentially technically oriented. When several audit tracks are supported by the same standards or a single audit is aimed to demonstrate compliance with eIDAS and BV requirements respectively, the attestation letter and/or conformity assessment certificate must ideally be separate. At the least such letters/certificates should express clearly, against which framework the assessed CA is conformant. Furthermore, the attestation report or certification (audit) report should also ideally be separate or at least include clear and consistent demonstration of the conformance with each of the targeted frameworks. It is worth noting that BVs refer to the "ETSI audit track", a technical track, as being accepted to support their decision of trust in the context of their trust framework, not the legal technology-neutral "eIDAS audit track" per se.

However, the bigger concern is about the consistency of audit criteria across SBs. An audit conducted by two different CABs accredited by two different SBs should produce the same results. BVs strongly support works towards harmonising the accreditation and certification schemes at the EU level, for CABs assessing (Q)TSP/(Q)TS

Transparency is a characteristic in which BV trust frameworks have invested. The more transparency the more a BV and other interested parties can be confident that a TSP is behaving according to the rules, is trusted and that BV users are protected. Certificate transparency, CA certificate disclosure requirements, publicly available CA data, publicly available non-conformities and publicly available incident and even CA audit reports are examples of tools and information required to be available to the public for use to monitor and improve the health of the CA ecosystem. Under eIDAS, none of this information is required to be public.

There is also a legitimately perceived lack of transparency in the current de facto adopted eIDAS accreditation (and certification) scheme in particular with respect to the following: the scope of the eIDAS certification scheme used by the eIDAS accredited CAB, the effective targeted criteria, the targeted audience, the corresponding assessments, including the tests performed of evaluated, their results, and the auditor's judgement or opinion on whether those results meet the stated objectives.

The lack of strong enforcement mechanisms in the eIDAS framework is also perceived by the BVs as an issue. CAs are required to notify their eIDAS accredited CAB whenever a non-conformity is identified but BVs reported having rarely, if ever, observed CABs and SBs taking apparent action/sanction against them. This may lead CAs to be comforted in making decisions favouring their own interests. Similarly, CABs issuing CAR reported to be of insufficient quality have not been (publicly) observed to be sanctioned by their competent NAB. Individual NABs are perceived by BVs to apply different level of rigor when overseeing CABs, which they accredited. On the contrary, WebTrust licensed practitioners are under a centralized governance model, believed by BVs to be a more consistent level of oversight than the eIDAS one, where CABs oversight is delegated to separate NABs from each EU MS.

BVs also believe the monitoring regime undertaken by CABs and by SBs is another area for improvement. Except for the initial and 2-yearly assessment of the risk management approach implied by eIDAS, the level of active monitoring exercised by CABs and SBs is unclear, not transparent and potentially inconsistent. On the opposite side, BVs' trust frameworks are almost exclusively focused on managing risk and protecting their users, for example by proactive actions, fast responses following active monitoring, or CA notified security issues (as BVs require). The lack of transparency regarding active monitoring of QTSP issuing qualified certificates as a QTS (and of other QTSP/QTS) may lead to the wrong perception by BVs that the eIDAS trust framework relies exclusively on audits. It is unclear to BVs (and probably not only to them) how factors such as CA's (QTSP's) competence, responsiveness and transparency when responding to an incident or CA's (QTSP's) fame or reputation or, credibility, or prior incidents are taken into account in the process of granting a qualified status.

In short, implementing mutual recognition is not part of the BVs' trust framework because they do not envisage surrendering their ability to enforce policies or requirements to CAs and their ability to exclude or distrust any non-conformant CA. The relationship between BVs and CAs is a direct one-to-one relationship-based BV-driven requirements imposed by each BV on each CA and is likely to remain so.

Better convergence and quicker alignment between the ETSI standards and the CA/Browser requirements driving all BV trust frameworks may be an additional area of improvement to foster convergence with the eIDAS framework, when supported by ETSI standards.

Furthermore, from a technical point of view, BV believe using TLS is not the only technical solution for implementing QWACs in accordance with the eIDAS Regulation. BVs reported that, in informal discussions with the EC, they suggested alternative technical solutions, other than using TLS, that could facilitate the recognition of QWACs. These technical solutions are based on the fact that Annex IV of the eIDAS Regulation does not require QWACs to include any "private key". QWACS could be implemented as "simple" signed or sealed attestations that a legal or natural person is linked to a domain name; such attestations could then be consumed, verified and/or displayed alongside the TLS connection. The technical feasibility, relevance, market adoption and standardisation of one or more of those alternative solutions still need to be progressed.

2.5.2 Adobe

Adobe has not provided any direct input to the context of the study. However, Adobe's AATL principles to the recognition of trustworthiness in certificate-based digital IDs and timestamp services are highlighted and assessed here by the study team for the interesting approach in a clean separation between a "legal" and "standard" processing of the EU Member States trusted lists and regarding them as trustworthy. In other words, on the one hand, considering the EU legal constitutive value of EU MS trusted lists[16] to validate qualified electronic signatures or seals and display the validation results in consequence. On the other hand, trusting those QTSPs issuing qualified certificates having been listed in the EUMS TL for being recognised as trustworthy as those CAs and TSPs having actively applied for and accepted in the Adobe Approved Trust List (AATL) program[17].

The AATL is a CA certificate trust store program that onboards certificate authorities (CAs) and trust service providers (TSPs) that demonstrated compliance with the AATL program requirements. The applicant CA must pass an audit from one of the audit schemes that are

[16] Called "EUTL" by Adobe, to clearly separate them from the "AATL".
[17] https://helpx.adobe.com/be_fr/acrobat/kb/approved-trust-list2.html

accepted by Adobe to support the vetting by Adobe that the applicant conforms to AATL requirements, namely:

- A compliance audit against [ETSI EN 319 411-1] NCP, [ETSI EN 319 411-2] QCP-n or QCP-l, conducted by an auditor that is accredited under the [ISO/IEC 17065] framework supplemented by [ETSI EN 319 403].
- A WebTrust™ for CA v2.0 or later conducted by a WebTrust™ licensed Practitioner for WebTrust™ audits.
- A compliance audit against [ISO 21188] conducted by an auditor that is accredited against [ISO/IEC 17065] for [ISO 21188] audits.

As an alternative[18] to the presentation of a conformity assessment report confirming the conformity against one or more of the above listed audit schemes specifications, demonstrating compliance with the AATL requirement can be achieved when the submitted CA "*is listed and granted a CA/QC qualified status in one of the European Member State national Trusted Lists (EUTL) as a qualified trust service for the issuance of qualified certificates for electronic signatures or electronic seals and the trusted list indicates directly, or indirectly through the certificate, that the certificate is stored on a Qualified Signature Creation Device"*.

Independently of an active application by a TSP/CA to the AATL program, Adobe digital signature solutions also work with every QTSP offering qualified trust services listed in the European Union Trust List (EUTL). Without the need for the corresponding QTSPs to apply for the AATL program, Adobe solutions validate all EU qualified electronic signatures and qualified electronic seals by processing the EU Member States trusted lists. The validation results are displayed in conformance with the eIDAS Regulation requirements for the validation of such signatures or seals (cf. Art.(32) of the Regulation), identifying if the signature/seal is supported by a qualified certificate, if the private key resides in a qualified signature/Seal creation device and hence if the signature is qualified under eIDAS.

In the study team's opinion, this illustrates in practice an interesting approach in a clean separation between processing the EU MS TLs and recognising them, or the underlying line of assessment, as trustworthy for joining the AATL program.

[18] Another alternative is for the applicant CA to meet the Medium Hardware Assurance Requirements of the US Federal Bridge, the SAFE-BioPharma bridge, or the CertiPath commercial bridge, by privilege of having the Supplied Certificate cross-certified to the bridge.

3. ANALYSIS OF THE AVAILABLE LEGAL FRAMEWORKS

3.1 INTRODUCTION

The eIDAS Regulation does not specify any particular accreditation scheme or any conformity assessment (or certification) scheme against which a CAB must be accredited and QTSP/QTSs be assessed. It limits itself to requiring the CAB to be accredited within the framework of Regulation (EC) No 765/2008 [Reg.765, 2008], and specifies the need for the execution of a conformity assessment scheme that is eIDAS specific - i.e. a scheme which confirms that, for a specific type of QTSP/QTS, a QTSP/QTS satisfies the applicable requirements of the eIDAS Regulation. However, the Regulation does not mandate EA to establish either a complete accreditation framework or certification schemes for each type of QTSP/QTS.

When looking at potential future actions aiming to establish a more comprehensive framework in relation to the auditing of QTSP/QTSs and working towards harmonising related EU certification schemes, three main approaches can be envisaged.

The first approach, within the current scope of the eIDAS Regulation, relates to the adoption of secondary legislation. Pursuant to Article 20(4) of eIDAS Regulation the European Commission may, by means of implementing acts, establish a reference number of standards on the accreditation of CABs, on CARs, and on auditing rules under which CABs will carry out their conformity assessment of QTSP/QTSs. The EC could by means of implementing Acts, establish reference number of standards allowing for presumption of compliance of QTSP/QTS with the applicable requirements of the eIDAS Regulation.

The 2020 revision of the eIDAS Regulation is the second approach that may be used to address the problem, by explicitly including references to relevant schemes and certification frameworks. A third promising approach that has recently become viable consists of the adoption of a certification scheme under the Cybersecurity Act [CyberAct, 2019]. The latter two options could be combined, by revising the eIDAS Regulation to clarify that the Cybersecurity Act may be used as an instrument to designate schemes that address the requirements of the eIDAS Regulation.

The next section explores these three different legal options available at the EU level to support a more harmonised approach to the certification of QTS/QTS.

3.2 eIDAS SECONDARY LEGISLATION

A proposal towards a more harmonised conformity assessment scheme for QTSP/QTS can be legally formalised through Article 20(4) of the eIDAS Regulation, which gives to 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".*

While the eIDAS Regulation thus permits the Commission to reference a scheme through an implementing Act, this path has not been used so far. The currently available candidate standards are [ETSI EN 319 403] and [ETSI TS 119 403-3], the latter building upon the first. It is worth noting the current version of [ETSI EN 319 403] suffers from some substantive issues[19] and is currently under revision. Those standards, after completing the revisions, would likely be good candidates for referencing under point (a) of Art.20(4).

However, none of those standards fully addresses the list of criteria, controls and control objectives an accredited CAB would use to conduct an assessment of the conformity of a QTSP/QTS with the eIDAS Regulation (cf. point (b) of Art.20(4)). So far, (European) standardisation bodies have developed no standard addressing such a list, which would allow CABs to assess the conformance of QTSP/QTS against the applicable eIDAS requirements, irrespective of the conformance of those QTSP/QTS with best practice technical standards. CEN/CENELEC and ETSI have however developed standards for such best practices, for each type of QTSP/QTS, with annexed tables mapping the requirements of the Regulation to the relevant clauses of the standards. However:

- No formal assessment of their suitability has been completed, particularly with the perspective of being referenced in an eIDAS implementing act.
- These are standards that QTSPs remain free to abide by or not; the standards are binding on the activities of CABs, not of the QTSPs.

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 way. In other words, the provision does not allow the EC to define itself the relevant specifications of an eIDAS QTSP/QTS conformity assessment (certification) scheme. At most, some of the requirements defined in a standard may be excluded from the reference in an implementing Act. So, when failures of candidate standards are identified during their eligibility assessments for being referenced by eIDAS implementing acts, those failures cannot be rectified through legislation. Rather, the problems would need to be notified to the competent standardisation organisations with a view of updating the standards accordingly and republishing them, and then referencing them as the legislation requires.

As a result, the adoption of an implementing Act pursuant to Article 20(4) would not, in the absence of standard(s) fully specifying a CAS, preferably created for each of the QTSP/QTS types, be an option to fully harmonise the auditing of eIDAS QTSP/QTS. However, referring to ETSI TS 119 403-3 (with revisions) in an implementing Act adopted pursuant to Article 20(4) would be a constructive step towards such harmonisation.

The EC could, by means of implementing Acts[20], establish reference numbers of standards allowing for presumption of compliance of QTSP/QTS with the applicable requirements of the eIDAS Regulation. This would contribute to reducing the diversity in the existing certification schemes, which have been defined by each individual CAB, by providing common roots for such schemes. However, the implementing Acts as foreseen by the eIDAS Regulation do not allow full coverage of the requirements applicable to QTSP/QTS for such presumption of

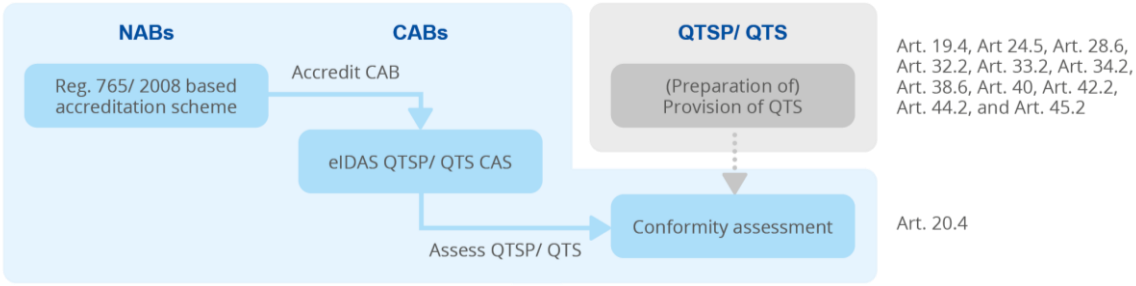
[19] When the decision to certify a QTSP/QTS is the confirmation that the assessed QTSP/QTS meet the applicable requirements of the eIDAS Regulation (i.e. the normative document, identified as the "product (read service) requirements" in ISO/IEC 17065), it shall not be possible to take such decision with pending non-conformities to these requirements, i.e. when the assessed QTSP/QTS actually fail to meet all the normative (eIDAS) requirements.
When a certification has been issued to a conformant QTSP/QTS (i.e. confirming that the assessed QTSP/QTS meets the requirements of eIDAS), and that a non-conformity with eIDAS requirements is substantiated, either as a result of surveillance or otherwise, it shall not be considered "an appropriate action" to maintain valid the certification (confirmation) that the certified QTSP/QTS is conformant, while there is still any unresolved non-conformity to the normative (eIDAS) requirements (i.e. when the assessed QTSP/QTS actually fail to meet all the eIDAS requirements).
[20] Namely, pursuant to Art.24(5), Art.27(4), Art.28(6), Art.32(3), Art.33(2), Art.34(2), Art.37(4), Art.38(6), Art.40, Art.42(2), Art.44(2), and Art.45(2).

compliance. This may moreover be a politically complex path. Despite prior initiatives from some EU MS, discussions on adopting such implementing Acts have not been initiated thus far.

The 2020 revision of the eIDAS Regulation is an opportunity that could be used to take account of the drawbacks of this first approach. For example, the EA, or another body, could be mandated to establish a complete accreditation framework and certification schemes for each type of QTSP/QTS, and to extend the coverage of other implementing Acts to all QTSP/QTS requirements as described above.

That revision may also be used to facilitate a third promising approach that has recently become viable to formalise an accreditation framework. This would consist in the adoption of a certification scheme under the Cybersecurity Act [CyberAct, 2019].

Figure 4: eIDAS secondary legislation as legal instrument toward harmonised CAS



Implementing acts (IAs) pursuant to eIDAS

Negative

- Not possible to achieve CAS harmonisation due to dependence on the existence and completeness of **standards**:
  - No existing standard on CAS
  - No mandate to EC to amend existing standards
  - No mandate to EC to define its own specifications
- Unclear legal effect to referencing standard under Art.20(4)
- Potentially politically complex path.

Positive

- Art.20.4 IA would allow to legally support EA recommended accreditation scheme based on EN 39 403 and extend it to CAS specifications (ST 119 403-3)
- Various other provisions permit adoption of IAs for each type of QTSP/QTS
- Reducing diversity in CABs' assessment schemes

3.3 THE CYBERSECURITY ACT

A key challenge – apart from agreeing on the definition of the requirements for a harmonised conformity assessment scheme for QTSs – is its formalisation as an official scheme with legal recognition across the EU. While the eIDAS Regulation could permit it to do so by referencing a scheme through an implementing act, this path has not been used so far. The Cybersecurity Act [CyberAct, 2019], which entered into effect on 27 June 2019, provides an alternative avenue.

The Cybersecurity Act, providing for a stronger and permanent legal mandate for ENISA, introduces a framework for the adoption of European cybersecurity certification schemes. The Cybersecurity Act allows the European Commission (or exceptionally the European Cybersecurity Certification Group established under the Act) to request ENISA to prepare a candidate certification scheme, which would apply to ICT products, services and processes.

The definition of these concepts is broad: notably, an '*ICT process*' is defined as "*a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service*". This could plausibly apply to a QTSP/QTS conformity assessment scheme, so that a harmonised scheme would be eligible for formalisation under the Cybersecurity Act.

The process of adoption involves several entities. If a request to ENISA to prepare a candidate scheme is issued, article 49 of the Act requires ENISA to consult relevant stakeholders through a formal, open, transparent and inclusive consultation process. In addition, ENISA must establish an ad hoc working group to finalise a candidate scheme; the results of the present report could act as a basis for this work. After consultation with the aforementioned European Cybersecurity Certification Group (ECCG), which is composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities, ENISA can submit its finalised candidate scheme to the European Commission, who may adopt it via an implementing Act under the Cybersecurity Act.

Once adopted, ENISA will publish the information on the certification scheme via ENISA's website. Furthermore, article 56 of the Act stipulates that any ICT products, ICT services and ICT processes that have been certified under an adopted scheme shall be presumed to comply with the requirements of such a scheme – which in the present case would relate to the security requirements for QTSPs/QTSs, mainly as dictated by the eIDAS Regulation.

The legal presumption of compliance, created by cybersecurity certification, with the targeted security requirements would nevertheless be subordinated to verification by the competent SB that the certified QTSP/QTS meets the eIDAS requirements, and to the SB's decision to grant a qualified status (or not) to the certified QTSP/QTS. In other words, certification is an element attesting to compliance with explicitly defined security requirements, but it does not automatically result in a qualified status being granted under the eIDAS Regulation.

Under the Cybersecurity Act, cybersecurity certification against a specific scheme approved under the Act is voluntary, since compliance with the certification scheme is not currently made mandatory by any existing legislation. Although this can of course change, depending on future developments of the eIDAS Regulation. QTSPs would therefore retain the possibility of demonstrating compliance with the law using any other method until legislation is introduced that changes this picture.

Crucially though, article 57 of the Act addresses the impact of adoption of schemes on any national cybersecurity certification schemes, stating that these "*shall cease to produce effects from the date established in the implementing act*", and that Member States are barred from adopting new national cybersecurity certification schemes with a scope covered by an EU level certification scheme. In other words, Member States would not be able to lend any legal value

to any national schemes that they may have defined in the application of the eIDAS Regulation. The notion of a "*national cybersecurity certification scheme*" is defined as "*a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme*" – i.e. it covers only requirements emanating from a public authority. Article 57 of the Cybersecurity Act thus has no impact on purely private sector schemes, or on schemes, which have not been formally adopted but are simply influential in practice.

The Act allows schemes to rely both on self-assessments and on formal certification. Support for self-assessments in a scheme is however not mandatory under the Act, and given current practices for QTSP/QTS, self-assessment does not seem to be in line with market expectations, or with the requirements of the eIDAS Regulation. A candidate scheme under the Act targeting conformity assessment for QTSPs/QTSs in all likelihood would therefore rely solely on certification. The process of certification must be elaborated in the scheme itself, but can be drafted to function in largely the same way as is done currently under the eIDAS Regulation.

The Act permits a scheme to contain several levels of assurance, ranging from 'basic' to 'substantial' and 'high', linked to the level of the risk associated with the intended use of the product, service or process, in terms of the probability and impact of an incident. Assuming that certification of QTSPs/QTSs would require a high level of assurance, Article 56.6 of the Act requires certificates to be issued by national cybersecurity certification authorities, which must be designated by the Members States. However, the national cybersecurity certification authorities may delegate this task to their CABs who are accredited by NABs under Regulation (EC) No 765/2008 to issue the required certificates. Therefore, the certification process would be highly comparable to current practice under the eIDAS Regulation.

As noted above, if QTSPs/QTSs are indeed expected to be certified under assurance level 'high' – which seems plausible – then Member States have the option of allowing certificates to be issued by their national cybersecurity certification authorities, who may not be accredited as CABs under Regulation (EC) No 765/2008. This would not be in line with the requirements of the eIDAS Regulation, which defines a CAB as "*a body defined in point 13 of Article 2 of Regulation (EC) No 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*". In other words, while Member States would have the option under the Cybersecurity Act to allow certificates to be issued by a national cybersecurity certification authority who is not itself a CAB, this would not be able to satisfy the requirements of the eIDAS Regulation. Therefore, the scheme should make it clear that any certificate issued under an adopted scheme must be issued by a CAB.

As a relevant nuance, it might be argued that the Cybersecurity Act focuses on cybersecurity, i.e. *the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats* (as defined in the Act); and not on legal compliance in general. Since CABs under article 20 of the eIDAS Regulation must confirm that the QTSPs and QTSs fulfil the requirements of the Regulation in general (and not only in relation to cybersecurity)[21], a scheme under the Cybersecurity Act risks not comprehensively covering the requirements of the eIDAS Regulation if it only focuses on the security elements.

The Act nevertheless stresses the need to adopt a broad and general notion of cybersecurity for the purpose of certification. While it imposes minimal contents for a scheme (notably mandatory

[21] In addition to security requirements specified in its Art.19, the eIDAS Regulation also comprises requirements on the scope and functionality of QTS, for QTSP operational continuity, staffing, liability, contractual transparency towards customers, and other QTS related elements, which have only an indirect link to cybersecurity.

security objectives and minimal elements to be included), the Act does not forbid explicitly the inclusion of other (non-security related) requirements. Therefore, it could be argued that the inclusion of non-security related elements in a scheme could be justified in case of qualified trust services, given that the objective of the eIDAS Regulation is to ensure that such services meet a high threshold of security and trustworthiness.

This would in practice imply that all requirements of the eIDAS Regulation could be integrated in a scheme. As such, an adopted security scheme under the Cybersecurity Act to streamline conformity assessment for QTSPs/QTSs would be very beneficial to reduce market fragmentation in relation to information security. It would then be recommended that this broad position would also be taken by the Commission when requesting schemes, or by ENISA (or its expert groups) when preparing a candidate scheme for harmonising QTSP/QTS certification of conformance with the requirements.

Figure 5: Cybersecurity Act as legal instrument toward harmonised CAS

3.4 eIDAS revision or amendment

Conceptually, an alternative process could also be to take the opportunity of the currently ongoing revision of the eIDAS Regulation to address specifically the establishment process, the specifications and maintenance of eIDAS QTSP/QTSs certification scheme(s).

Under this option, article 20 of the eIDAS Regulation could be rewritten in a manner that makes it clear that the scheme creation process envisaged under the Cybersecurity Act should not be limited to information security aspects but could also be used to establish comprehensive QTSPs/QTSs certification scheme(s). It could clarify that the contents of such schemes should consider the entirety of the eIDAS Regulation requirements as being relevant to supporting the security of QTSPs/QTSs. In that way, it would be unambiguously clear that, in the context of the eIDAS Regulation, the Act is a suitable and viable avenue for establishing the required schemes. It is worth noting that, from a legal point of view, whether this would be at all possible would depend on the scope of the Cybersecurity Act. Indeed, the eIDAS Regulation cannot amend this Act.

Alternatively, if the Cybersecurity Act would not be considered a valid option, the 2020 revision of the eIDAS Regulation may be used to compensate the drawbacks of the first approach, by mandating EA. A standardisation body, or another body entitled to play the role of scheme owner, to establish a complete accreditation framework and certification schemes for each type of QTSP/QTS. It may also present the opportunity to extend the coverage of other implementing acts to all QTSP/QTS requirements.

4. GAP ANALYSIS – TOWARD A HARMONISED SCHEME

4.1 GENERAL PRINCIPLES

4.1.1 eIDAS Regulation driven

A CAR needs to demonstrate the fulfilment of each applicable eIDAS requirement. Therefore, an EU-wide harmonised conformity assessment scheme would start from the eIDAS requirements for QTSP/QTS, with a common part for all types of QTS together with specificities for each, then detailing controls and control objectives about them.

4.1.2 In-depth list of controls and control objectives

Because the eIDAS requirements are legal high-level requirements, the scheme shall identify as detailed as possible technical/operational criteria and criteria objectives concerning each of these applicable eIDAS requirements that can serve as a basis for audits. Information and guidance for this identification may be taken from:

- ETSI / CEN standards relevant to support the implementation of the eIDAS Regulation.
- ENISA guidelines, in particular guidelines mapping the above standards to the eIDAS requirements and identifying remaining gaps.
- Nationally-defined schemes (e.g. from Slovakia, Czech Republic, or France) and private sector schemes (e.g. UK tScheme). It should be noted that these schemes have shown to be conflicting in some aspects, and the definition of an EU-wide scheme should take these issues into consideration.
- Being supplemented for identified gaps by more “generic” standards such as ISO/IEC 27001, ISO/IEC 27701 or other legal frameworks such as GDPR for data protection.

4.1.3 Technological neutrality – QTSP freedom of implementation

The outcome of the definition of criteria and criteria objectives described above could lead to checklists aiming to support efficiently the CAB in assessing the conformity of a QTSP/QTS against the eIDAS Regulation. Setting up these checklists will be a challenge, as they will have to meet conflicting objectives:

- Being specific and detailed enough to enable a clear and precise assessment of the conformity of a QTSP/QTS against the eIDAS Regulation, and its demonstration.
- Being generic enough to be technology-neutral, as eIDAS aims to be. It is worth noting that the above-mentioned standards were drafted first as standardized requirements for specific PKI-based implementations of QTSP/QTS, providing less guidance or no guidance at all for the audit of “alternative” or “creative” implementations of the eIDAS requirements. The same applies to the above-mentioned ENISA guidelines and nationally-defined or private schemes, that all rely, with some variances, on those standards. These standards should remain “one possible path” of implementing the eIDAS requirements.

For ease of use, one checklist would be identified for each QTS, and potentially for each relevant “component” service.

4.1.4 Specific Member State requirements

Because some requirements are left open[22] by the eIDAS Regulation and specific to each country (e.g. suspension of certificates, video onboarding), the resulting checklists should take into account these specificities depending on which country of Europe the QTSP is established in, and allow the possibility to refer to “conditional controls” for each.

It is worth noting that it is key to limit national specificities to aspects explicitly identified by the eIDAS Regulation as nationally specific, in order to limit the possibilities of divergence.

4.1.5 Scheme owner & maintenance

Once established, this EU-wide eIDAS QTSP/QTS certification scheme shall be maintained appropriately to ensure it remains fit for purpose in the long run.

A continuous improvement process shall be defined for such scheme, and shall include the definition of a scheme management authority (i.e. scheme owner), an EU-wide representative working group and a review process.

4.2 MULTIPURPOSE AUDITS

The process towards the definition of harmonised QTSP/QTS certification schemes should take into consideration that some QTSPs might operate in an international environment and in this regard, they may need to be audited for other purposes than eIDAS compliance. The usual example cited by stakeholders relates to the CA/Browser Forum[23] requirements. However, another case for multipurpose audits deals with the potential certification of information security management systems (ISMS) and privacy information management systems (PIMS) used by QTSP to provide QTS. QTSPs may benefit from prior audit focussing on these aspects (e.g. against ISO/IEC 27001 and/or ISO/IEC 27701) or be keen to obtain related certifications. It must be stressed however that to be relevant to eIDAS, the respective statements of applicability (scope) of these ISMS and PIMS must address the provision of QTS by QTSP. In this context, it would be key to make sure the EA recommended eIDAS accreditation scheme would allow eIDAS accredited CABs to conduct those side audits and certifications.

An acceptable certification scheme should support multi-purpose audits wherever possible to avoid QTSPs undergo multiple audits. To that extent, it should be noted that such multi-purpose audits shall need to result in as many different CARs / audit reports and certification decisions as there would be “Normative Documents” against which the conformity of QTSP/QTS should be confirmed.

It is of paramount importance to consider that CARs in the context of Articles 21.1, 20.1 and 20.2 of the eIDAS Regulation shall confirm the conformity of QTSP/QTSs to the requirements of the eIDAS Regulation and not to any standard. Yet, in practice, standards may be of great help for TSPs to ensure best practices, and of great help for CABs in their activities of assessing these TSPs claiming compliance to the standard or the normative document, in particular when the CAB they select is building its eIDAS certification scheme upon identified standards.

[22] These requirements are not “open” in the sense that they are voluntary. But in order to achieve a certain objective, Member States enjoy the freedom to choose different means. The use of video for onboarding when issuing qualified certificates for instance (cf. point (d) of Art.24(1)), if confirmed by an eIDAS accredited CAB as being equivalent in terms of reliability to physical presence of the person to whom the certificate is issued.
[23] https://cabforum.org/

4.3 COMPOSITE AUDITS IN THE CONTEXT OF eIDAS REGULATION

As has been explained in the feedback from CABs and SBs, composite audit is a key concept to take into account in the definition of harmonised eIDAS QTSP/QTS certification scheme(s).

When appropriately applied, it may save significant effort (by QTSPs and by CABs) and, simultaneously, retain the assurance level of conformity assessment. It is key to design the composite certification approach in a way which ensures no decrease in the assurance level of the assessment result and no distortion of the competition between CABs.

4.4 INTERNATIONAL ASPECTS

In addition to the international aspect resulting from the need for QTSP/QTS to meet other (international) compliance schemes, the international promotion and recognition of the eIDAS auditing model (accreditation of CABs under eIDAS and QTSP/QTS certification scheme(s) used by eIDAS accredited CABs) are key elements for:

- Facilitating international mutual recognition foreseen in Article 14 of the eIDAS Regulation.
- Expanding eIDAS accredited CABs' market from EU to international.

The IAF MLA driven accreditation scheme based on ISO/IEC 17065 (ideally to be supplemented by ETSI EN 319 403-1) is a very natural and interesting candidate for 3rd countries to base their national QTSP/QTS certification scheme on, particularly for QTS other than issuing qualified certificates. Promoting ETSI EN 319 403-1 at ISO level would also be an alternative to envisage.

4.5 ISO/IEC 17067

With [ISO/IEC 17065] being the cornerstone for the EA recommended scheme, a good policy choice would be to develop EU-wide harmonised eIDAS certification schemes based on the recommendations of [ISO/IEC 17067].

4.6 LEGAL INSTRUMENTS

It is unclear at this stage which legal instrument(s) would actually be selected to reference or establish future EU harmonised eIDAS certification scheme(s) for QTSPs/QTSs. As argued above, the Cybersecurity Act could be an appropriate avenue, if its provisions are given a broad interpretation so that all requirements of the eIDAS Regulation could be covered as being relevant to security (rather than only those that are explicitly and exclusively targeting security requirements in the strictest sense).

Whatever option is chosen, it would be key that the design process of such schemes would be conducted in such a way to federate, consult and involve as many relevant types of stakeholders (or representatives) through a formal, open, transparent and inclusive consultation process.

5. RECOMMENDATIONS

5.1 OVERVIEW

Based on the stakeholders' collected input, on the current eIDAS regime and the analysis of the present report, action should be taken as proposed hereafter. The goal is to meet stakeholders' concerns and legitimate needs to move towards a more harmonised approach with regards to the assessment by CABs of the conformity of QTSP/QTSs with the requirements of the eIDAS Regulation.

5.2 ACTIONS REGARDING LEGAL INSTRUMENTS TOWARDS AN EU HARMONISED eIDAS CAS

Note: The entity responsible for taking LEG-x recommendations forward is the European Commission (either autonomously under the eIDAS Regulation, or by granting a mandate to ENISA and then formalising the outcome under the Cybersecurity Act).

LEG-1. The track offered by the Cybersecurity Act is suggested to be the favoured option concerning the creation of a harmonised certification scheme for each of the (nine) types of QTSP/QTS specified in the eIDAS Regulation.

Additional certification schemes could also be created to cover the need to assess/audit QTSP service components or processes in the context of Annex II.3 & 4 and in the context of implementation of Art.24.1(d) of the eIDAS Regulation.

As this might be a lengthy process, the currently available mechanism of adopting implementing Acts under the eIDAS Regulation could be used to:

LEG-2. Reference the ETSI TS 119 403-3 standard pursuant to Art.20.4 of the Regulation to address both points (a) and (b) of Art.20.4. The eligibility of that standard for such a referencing should be formally assessed. It is currently conditioned to the replacement of its normative reference towards EN 319 403 by a normative reference to EN 319 403-1 where this standard updates of the current version of EN 319 403 to prevent CABs to issue (or maintain valid) certificates of conformity with non-conformities to the eIDAS Regulation.

This adoption would not fulfil the need for a harmonised CAS but at least would formalise the recognition of the current recommended EA eIDAS accreditation scheme. It would also clarify the requirement for CABs accredited under this scheme to have a suitable and appropriate CAS leading to the production of a CAR fulfilling a minimum set of requirements largely demanded by EU MS SBs.

LEG-3. Reference formally assessed appropriate standards regarding (Q)TSP and the QTS they provide, in particular pursuant to Art.19.4, Art.24.5, Art.28.6, Art.32.2, Art.33.2, Art.34.2, Art.38.6, Art.40, Art.42.2, Art.44.2, and Art.45.2.

It is a fact that such referencing may not confer to these standards a presumption of compliance to the entire set of the eIDAS requirements applicable to each type of QTSP/QTS. However, this may lower significantly the level of uncertainty on the side of QTSPs, and remove barriers to QTS market development and adoption.

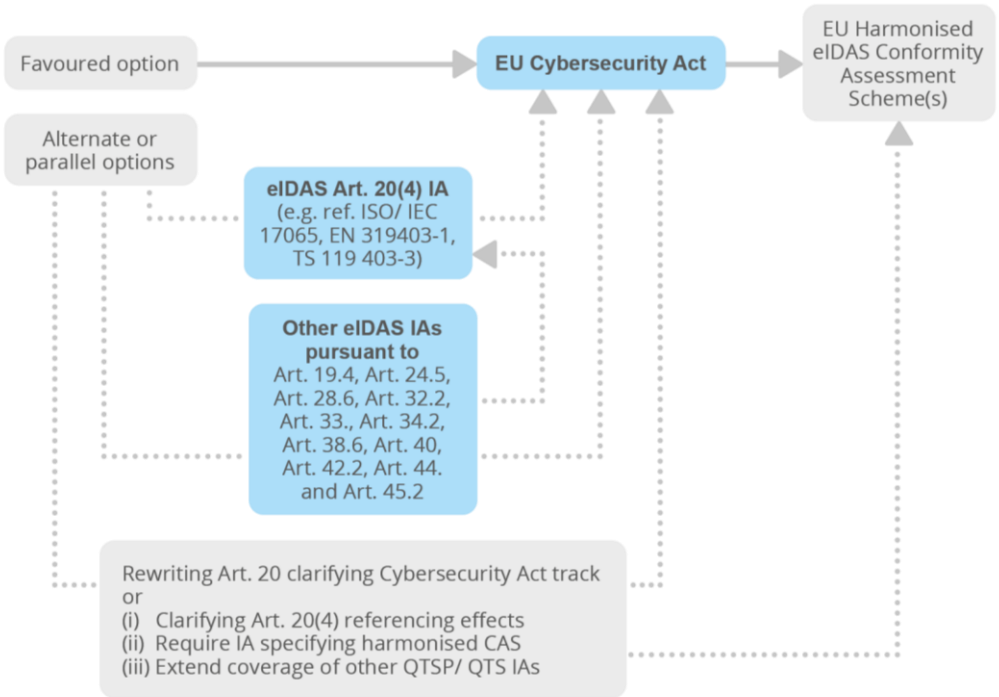
In the absence of harmonised CAS(s), such adoptions may also facilitate the work of the CABs and contribute to increasing the number of CABs accredited to assess more types of QTS.

Adopting such implementing Acts has however revealed to be a quite lengthy and uncertain process as so far, none of the above-mentioned Acts has been adopted despite numerous attempts from EU MSs to have such adoption process started. It is also subject to the eligibility of the current standards to be referenced and to the impossibility to amend those standards by means of the implementing Act when parts would need to be changed. The current shape of the Regulation does not give the mandate to the Commission to do so or to create the specifications itself. So, when failures of candidate standards are identified during the eligibility assessments, those would need to be notified to the competent standardisation organisations for updating the standards accordingly and republishing them.

LEG-4. In the context of Art.49 review of the application of the eIDAS Regulation, and as the deadline for the related review report is approaching (01.07.2020), for potential proposals for improvement, it is advisable to consider modifying the scope or the specific provisions of the Regulation:

a. If the Cybersecurity Act track is an option, rewrite Article 20 of the eIDAS Regulation, e.g. in a manner that makes it clear that the scheme creation process envisaged under the Cybersecurity Act should not be limited to information security aspects but could also be used to establish QTSP/QTS certification scheme(s). It could clarify that the contents of such schemes should consider the entirety of the eIDAS Regulation requirements as being relevant to supporting the security of QTSP/QTS. In that way, it would be more unambiguously clear that the Act is a suitable and viable path for establishing the required schemes.
b. In the absence of such an option:
    i. Consider clarifying the mandatory aspect of standards referenced under Art.20.4 of the eIDAS Regulation.
    ii. Require the adoption of an implementing Act specifying a harmonised CAS for each of the types of QTSP/QTS specified by the Regulation, covering the confirmation that certified QTSP/QTSs meet all applicable requirements of the Regulation. CAS should be added for assessing/auditing QTSP processes in the context of Annex II.3 & 4 and in the context of implementation of Art.24.1(d).
    iii. Extend current implementing Act coverage to all applicable requirements of the Regulation for each of the types of QTSP/QTS specified in the Regulation.

Figure 7: Flow of legal actions toward EU Harmonised eIDAS CAS(s)



5.3 ACTIONS REGARDING THE DESIGN OF EU HARMONISED QTSP/QTS CAS

Note: The entity responsible for taking all of the CAS-x recommendations forward is/are the body(ies) that will be assigned the task to develop EU harmonised CAS within the selected legal approach.

Irrespective of the chosen legal instrument, EU harmonised CASs should be established for each of the (nine) types of QTSP/QTS and for assessing/auditing QTSP component service or processes in the context of Annex II.3 & 4 and of Art.24.1(d). These CASs should be designed in accordance with the following recommendations:

CAS-1. Include the harmonised CAS(s) in an accreditation framework based on ISO/IEC 17065, supplemented by EN 319 403-1 and by TS 119 403-3;

CAS-2. Design the harmonised CAS(s) in accordance with ISO/IEC 17067;

CAS-3. Design the harmonised CAS(s) to be suitable and efficient in confirming that the assessed QTSP/QTS is meeting the applicable requirements of the eIDAS Regulation. For example, specifying sufficient concrete requirements, criteria, criteria objectives, checks and tests, to be used by the CAB to conduct the assessment of QTSP/QTS against the eIDAS Regulation;

CAS-4. Structure the assessment and assessment reporting in accordance with the list of requirements (following the numbering of the articles) of the Regulation while mapping them with the list of criteria and criteria objectives, the checks, tests and evaluations the CAB shall conduct to demonstrate the assessed QTSP/QTS meet the corresponding requirements;

CAS-5. Identify as detailed as possible technical/operational criteria and criteria objectives about each of these applicable eIDAS requirements that can serve as a basis for audits. Information and guidance for this identification may be taken from relevant ESO standards, ENISA guidelines, nationally defined and/or private sector schemes;

CAS-6. Leverage on the existing relevant standards whose technical compliance is aimed to facilitate the demonstration of QTSP/QTS compliance with the eIDAS Regulation requirements (e.g. CEN/CENELEC & ETSI EN/TS x19 xxx standards, ISO/IEC 27001, ISO/IEC 27701);

CAS-7. Leverage on the existing conformance testing facilities provided by ESOs and/or, by the EC (e.g. CEF building blocks reference implementations or testing facilities), that are suitable to support the conformance of implementation of QTSP/QTS with the eIDAS Regulation requirements;

CAS-8. Design the harmonised CAS(s) in a way not hindering the technology neutral approach of the eIDAS Regulation and leaving QTSP free to select the technical standards of their choice. Allow for alternative controls/measures exhibiting equivalent assurance and security;

CAS-9. Provide guidance (or requirements) on the minimum audit time and effort for completion of full assessments and surveillance assessments. This guidance (or the requirements) would aim to ensure a sufficient level of quality and bring credibility to the assessment outcome. Factors include the audit time for completion of full assessment, the level of expert-knowledge of the auditor/audit team, efficient audit procedures and used tools for automation of audits;

CAS-10. Allow the harmonised CAS to be combined with other-purpose assessments (e.g. ISMS, PIMS, CA/Browser Forum) and ensure that for multi-purpose certification

schemes, it is requested to make use of as many distinct declarations (attestations) of conformity as there are identified purposes;

CAS-11. Allow for the inclusion of requirements defined at national level, when and only when such national specificities are foreseen or allowed by the eIDAS Regulation. For example, suspension rules for qualified certificates for electronic signatures and/or for electronic seals, and identification of persons in the context of Article 24.1(d) of the Regulation.

CAS-12. Allow for composite certification, and handling of composite audits, where components (and/or processes) of a QTS are audited separately by different CABs, in a way that

a. Service component certification schemes are designed separately or clearly identified in the corresponding QTS certification scheme allowing distinct QTS components to be assessed independently with the aim of an appropriate aggregation to support the assessment of the overall QTS, without having to repeat a full assessment of all components again.
b. CABs can take into considerations earlier audit reports/certification decisions when performing the assessment of a QTSP/QTS.
c. Rules for accepting existing and underlying certification are clearly established[24].
d. The certification of “Remote QSCD operation and management”, of “(Q)TS factory services”, of “registration authorities” and in particular the certification of "remote identification procedures" foreseen in Art.24.1(d) of eIDAS are amongst the first composite certification schemes needed.

CAS-13. Consider harmonising surveillance activities and their periodicity.

5.4 CAS OWNER(S)

Once established, the EU-wide eIDAS QTSP/QTS certification schemes should be maintained appropriately (including in a transparent, consistent, and agile way) to ensure they remain fit for purpose in the long run.

A continuous improvement process shall be defined for such scheme. This implies the designation of a scheme management authority (i.e. scheme owner), of an EU-wide representative working group and the design of a review process. The working group should include relevant stakeholders, including NABs (potentially represented by EA), EA, EU MS representatives (e.g. members of the eIDAS experts group), EU MS SBs, FESA, each and every eIDAS accredited CAB and candidate CABs, independent experts and/or academics, ESOs, QTSPs and ENISA. In particular, rules must be defined for:

- Maintaining the scheme(s)
- Providing documented guidance on how to apply it(them)
- Dealing with new situations encountered by CABs and/or SBs and consequently providing/updating guidance on how to apply the scheme in consequence.

5.5 “QUICK WINS”

Note: The responsible entity for taking each QW-x recommendation forward is the individual entity mentioned in each of the respective sections (ETSI, EA or CABs).

The following quick wins should be implemented as of now:

QW-1. ETSI to be advised

a. to provide the appropriate corrections to ETSI EN 319 403 when updating it under EN 319 403-1 (see section 3.3)

[24] See section 2.3.4

b. to update TS 119 403-3 to normatively refer to EN 319 403-1 instead of referring to EN 319 403.

QW-2. EA to be advised

a. to update its recommended eIDAS accreditation scheme to ISO/IEC 17065, supplemented by ETSI EN 319 403-1 and by ETSI TS 119 403-3 in an updated version to refer to EN 319 403-1.
b. to clarify towards its members (i.e. the NABs):
    i. the wording to be used in order to indicate the scope of the accreditation of CABs in the context of eIDAS. Clear guidance should be provided for each of the nine types of QTS specified by the eIDAS Regulation.
    ii. the need to include in the eIDAS accreditation attestation or certificate issued to a CAB, the location where the corresponding accredited conformity assessment scheme (or certification scheme) is available for each type of QTS the CAB is accredited for conducting audits against the eIDAS Regulation.
    iii. the need to ensure the provision of historical information regarding the grant of the accreditation on a per QTSP/QST type basis.
    iv. the need to provide an indication, when the EA recommended eIDAS accreditation scheme is not used or not entirely used, that the alternative scheme used has been determined equivalent and under which basis.
c. To promote the eIDAS recommended accreditation scheme to the IAF level (see section 4.4).

QW-3. Currently accredited eIDAS CABs to be advised

a. to request extending the scope of their eIDAS accreditation to ETSI TS 119 403-3, as they may already do so towards their competent NAB.
b. not issuing eIDAS QTSP/QTS certification of conformity with the eIDAS Regulation as long as there exist non-conformities to this Regulation[25].
c. for multi-purpose certification schemes, to make use of as many distinct declarations (attestations) of conformity as there are identified purposes.

QW-4. All eIDAS accredited CABs to be advised to create a CAB cooperation working group gathering each and every eIDAS accredited CAB, as well as candidates, on a free of charge and automatic (or voluntary) basis, all having equal voice and vote. This group would aim to facilitate harmonization of the application of eIDAS QTSP/QTS conformity assessment schemes, approaches and criteria. It would be key as well for this group to cooperate tightly with SBs (e.g. FESA, EU MS eIDAS expert group members), ENISA and the European Standardisation Organisations.

[25] This would actually be illegal under the eIDAS Regulation.

6. BIBLIOGRAPHY/REFERENCES

6.1 REFERENCES

ID	Description
ANSSI, 2017	Organismes d'évaluation de la conformité des prestataires de service de confiance. Critères de reconnaissance au titre du règlement eIDAS. Available from http://www.ssi.gouv.fr.
COFRAC, 2019	Exigences spécifiques pour l'accréditation des organismes procédant à la certification des prestations liées à la sécurité des systèmes d'information. CERT CPS REF 33. Available from http://www.cofrac.fr. https://tools.cofrac.fr/documentation/CERT-CPS-REF-33
CyberAct, 2019	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) https://eur-lex.europa.eu/eli/reg/2019/881/oj
DKPv2	Ministry of Interior of the Czech Republic, A document specifying the requirements for qualified providers of trust services and their qualified trust services, version 2i, 12.03.2018. https://www.mvcr.cz/mvcren/ViewFile.aspx?docid=22021696
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 27001	ISO/IEC 27001:2013: "Information technology -- Security techniques -- Information security management systems -- Requirements".
ISO/IEC 27701	ISO/IEC 27701:2019: “Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines”.
NSA - CS	NSA, Certifikačná schéma pre eIDAS, Verzia 0.3 http://ep.nbu.gov.sk/kca/tsl/CertifikacnaSchemaNBU.pdf
MSA-CP/05	MSA-CP/05: Application of ETSI EN 319 403 v2.2.2 (2015-08) by assessment of CAB certifying products according to eIDAS. http://www.snas.sk/index.php?l=en&what=1&s=2&id=114
PASSI	Prestataire d’audit de la sécurité des systèmes d’information, référentiel d’exigences. Available from http://www.ssi.gouv.fr.
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
SK Act 272	Act No 272/2016 Coll. on trust services for electronic transactions in the internal market and on the amendment and supplementing of certain acts (act on trust services). https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272

6.2 BIBLIOGRAPHY

6.2.1 Applicable legislations

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
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
CID (EU) 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. OJ L 235, 9.9.2015, p. 26–36. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D1505
Reg.881, 2019	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). OJ L 151, 7.6.2019, p. 15–69. https://eur-lex.europa.eu/eli/reg/2019/881/oj

6.2.2 ETSI standards applicable to (Q)TSP/(Q)TSs

Source: ETSI TS 119 403-3.

Qualified trust service in Regulation (EU) No 910/2014	Standards
Provision of qualified certificates for electronic signatures	ETSI EN 319 411-2 (requiring compliance with ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412-2, ETSI EN 319 412-5)
Provision of qualified certificates for electronic seals	ETSI EN 319 411-2 (requiring compliance with ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412-3, ETSI EN 319 412-5)
Provision of qualified certificates for website authentication	ETSI EN 319 411-2 (requiring compliance with ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412-4, ETSI EN 319 412-5)
Provision of qualified time stamps	ETSI EN 319 421 (requiring compliance with ETSI EN 319 401), ETSI EN 319 422
Qualified validation service for qualified electronic signatures	ETSI TS 119 441 (requiring compliance with ETSI EN 319 401), ETSI TS 119 442, ETSI EN 319 102-1, ETSI TS 119 102-2 ETSI TS 119 172-4
Qualified validation service for qualified electronic seals	ETSI TS 119 441 (requiring compliance with ETSI EN 319 401), ETSI TS 119 442, ETSI EN 319 102-1, ETSI TS 119 102-2 ETSI TS 119 172-4
Qualified preservation service for qualified electronic signatures	ETSI EN 319 401, ETSI TS 119 511, ETSI TS 119 512
Qualified preservation service for qualified electronic seals	ETSI EN 319 401, ETSI TS 119 511, ETSI TS 119 512
Qualified electronic registered delivery services	ETSI EN 319 401, ETSI EN 319 521, ETSI EN 319 522 ETSI EN 319 531, ETSI EN 319 532

References and other relevant standards

ID	Description
TS 119 101	ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".
TS 119 102-1	ETSI TS 119 102-1 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".
TS 119 102-2	ETSI TS 119 102-2: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report".
EN 319 122	ETSI EN 319 122 series: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: "Building blocks and CAdES baseline signatures". Part 2: "Extended CAdES signatures".
EN 319 132	ETSI EN 319 132 series: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: "Building blocks and XAdES baseline signatures". Part 2: "Extended XAdES signatures".
EN 319 142	ETSI EN 319 142 series: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: "Building blocks and PAdES baseline signatures".

	Part 2: "Additional PAdES signatures profiles".
EN 319 162	ETSI EN 319 162 series: Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: "Building blocks and ASiC baseline containers". Part 2: "Additional ASiC containers".
TS 119 172	ETSI TS 119 172 series: Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: "Building blocks and table of contents for human readable signature policy documents"; Part 2: "XML Format for signature policies"; Part 3: "ASN.1 Format for signature policies"; Part 4: "Signature validation policy for European qualified electronic signatures/seals using trusted lists".
EN 319 401	ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
EN 319 403	ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".
TS 119 403-2	ETSI TS 119 403-2: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates".
TS 119 403-3	ETSI TS 119 403-3: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers".
EN 319 411-1	ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
EN 319 411-2	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".
TR 119 411-4	ETSI TR 119 411-4: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against EN 319 411-1 or EN 319 411-2".
EN 319 412-2	ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".
EN 319 412-3	ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".
EN 319 412-4	ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".
EN 319 412-5	ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QcStatements".
EN 319 421	ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
EN 319 422	ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
TS 119 431-1	ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".
TS 119 431-2	ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".
TS 119 441	ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".
TS 119 442	ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services".

TS 119 511	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 general data using digital signature techniques".
TS 119 512	ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services".
EN 319 521	ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".
EN 319 522	ETSI EN 319 522 series: Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: "Framework and Architecture"; Part 2: "Semantic contents"; Part 3: "Formats"; Part 4: "Bindings": Sub-part 1: "Message delivery bindings"; Sub-part 2: "Evidence and identification bindings"; Sub-part 3: "Capability/requirements bindings".
TS 119 524	ETSI TS 119 524 (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services".
EN 319 531	ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".
EN 319 532	ETSI EN 319 532 series: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: "Framework and Architecture"; Part 2: "Semantic contents"; Part 3: "Formats"; Part 4: "Interoperability profiles".
TS 119 534	ETSI TS 119 534 (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services".
TS 119 612	ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".
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".
TS 419 261	CEN TS 419 261: Security requirements for trustworthy systems managing certificates and time-stamps.

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