EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CONFORMITY ASSESSMENT OF QTPS

Technical guidelines for conformity assessment of qualified trust service providers

MARCH 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally 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 support to this report. ENISA would also like to thank the contributors to the first set of recommendations in this area, whose work was the basis of this work.

LEGAL NOTICE

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

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-437-4 - DOI: 10.2824/785453

TABLE OF CONTENTS

ABBREVIATIONS

CA	Certification Authority
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CAS	Conformity Assessment Scheme
CEN	Centre Européen de Normalisation
CID	Commission Implementing Decision
EA	European cooperation for Accreditation
EC	European Commission
EN	European Standard
ETSI	European Telecommunications Standards Institute
ETSI ESI	ETSI (Technical Committee) Electronic Signatures and Infrastructures
ETSI TS	ETSI Technical Specifications
EU	European Union
GDPR	General Data Protection Regulation
ISMS	Information Security Management System
ISO	International Organization for Standardisation
MLA	Multi-Lateral Agreement
MS	Member State
PIMS	Privacy Information Management System
PKI	Public Key Infrastructure
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
	Note: This may refer to a TSP intending to become a QTSP for the provision of a QTS
QWAC	Qualified Website Authentication Certificate
SB	Supervisory Body
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

To promote the use and further enhance the trust of electronic trust services and products, Regulation (EU) N°910/2014, on electronic identification and trust services for electronic transactions in the internal market [eIDAS, 2014], introduces the notions of qualified trust service (QTS) and qualified trust service provider (QTSP) with a view to setting out the requirements and obligations that ensure high-level security of QTS provision and of the products (devices) and processes used by QTSPs to provide these services in accordance with the Regulation. As a consequence, eIDAS QTS are granted a higher presumption of their legal effect.

A key policy choice made by the eIDAS Regulation is that, in order to be granted a qualified status by a national supervisory authority, trust service providers (TSPs), and the QTSs they plan to provide, must first demonstrate that they meet the functional requirements of the Regulation. This implies that TSPs and the QTSs they intend to provide need to undergo a specific process and receive a ‘green light’ from a competent national supervisory body (SB), which verifies they meet the requirements. If successful, this process then leads to their inclusion in the national trusted list confirming their qualified status.

As part of this process, the prospective QTSP/QTS must be audited by an eIDAS accredited conformity assessment body (CAB) to verify, through a conformity assessment (audit) report (CAR), that they meet the requirements of the eIDAS Regulation. The CAB needs to be accredited by a national accreditation body (NAB) in line with Regulation (EU) 765/2008 on the basis of a conformity assessment scheme (CAS) that is suitable for assessing the compliance QTSPs and the QTSs they provide (hereafter QTSPs/QTSs) with the eIDAS requirements.

Once granted a qualified status, a QTSP/QTS, must undertake at least every two years an assessment to confirm that the QTSP/QTS continue to meet the requirements of the eIDAS Regulation (see Art. 20.1 of eIDAS). Furthermore, the competent SB may at any time audit or request a conformity assessment body to perform a conformity assessment of the QTSPs, at the expense of those trust service providers, to confirm that they and the QTSs provided by them fulfil the requirements laid down in the eIDAS Regulation (see Art. 20.2 of eIDAS).

This document provides an overview of the conformity assessment framework for QTSPs as set out in the eIDAS Regulation, i.e. aiming to confirm that the assessed QTSP/QTS fulfils its requirements. This report discusses the typical process flow and the methodology used to perform conformity assessments. For each phase of the assessment, guidance is provided to QTSPs for the purpose of preparing and undertaking the conformity assessment, as required by the eIDAS Regulation, in the best possible conditions.

.

1. INTRODUCTION

1.1 THE EIDAS CONFORMITY ASSESSMENT FRAMEWORK

1.1.1 eIDAS requirements for conformity assessments of QTSPs

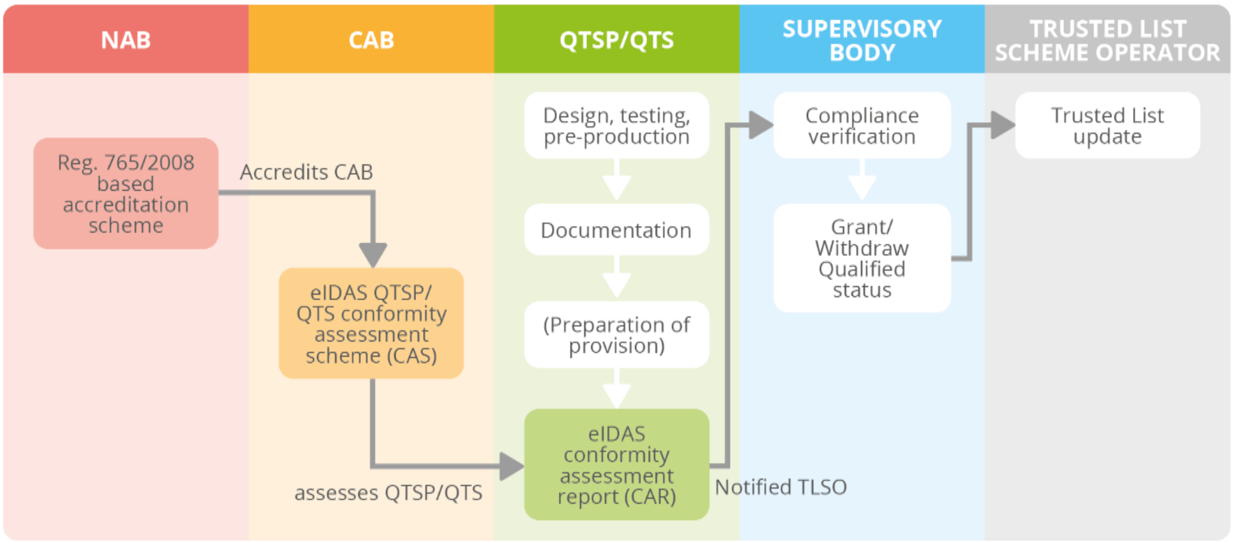
To further enhance the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market, and to promote the use of trust services and products, Regulation (EU) N°910/2014, on electronic identification and trust services for electronic transactions in the internal market [eIDAS, 2014] (hereinafter eIDAS Regulation), introduces the notions of qualified trust service (QTS) and qualified trust service provider (QTSP) with a view to setting out the requirements and obligations that ensure high-level security of QTS provision and of the products (devices) and processes used by QTSPs to provide these services in accordance with the Regulation. As a consequence, eIDAS QTS are granted a higher presumption of their legal effect.

A key policy choice made by the eIDAS Regulation is that, in order to be granted a qualified status by a national supervisory authority, trust service providers (TSPs) must first demonstrate that they and the QTSs they plan to provide meet the functional requirements of the Regulation. This implies that TSPs and the QTSs they intend to provide need to undergo a specific process and receive a ‘green light’ from a competent national supervisory body (SB) to attest to their conformity with the requirements. If successful, this process then leads to their inclusion in the national trusted list attesting their qualified status.

As part of this process, the prospective QTSP/QTS must be audited by an eIDAS accredited conformity assessment body (CAB) to confirm, through a conformity assessment (audit) report (CAR), that they meet the requirements of the eIDAS Regulation. The CAB needs to be accredited by a national accreditation body (NAB) in line with Regulation (EU) 765/2008 on the basis of an eIDAS suitable conformity assessment scheme (CAS) and CAB’s competence for assessing the compliance QTSPs and the QTSs they provide (hereafter QTSPs/QTSs) with the eIDAS requirements.

As the next step of the process, the prospective QTSP notifies its intention to provide QTS to its competent national 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 whether to grant a qualified status or withdraw an existing qualified status. Even in the event of a positive CAR, supervisory bodies may decide not to grant the qualified status.

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


NAB
CAB
QTSP/QTS
SUPERVISORY BODY
TRUSTED LIST SCHEME OPERATOR
Reg. 765/2008 based accreditation scheme
Accredits CAB
eIDAS QTSP/ QTS conformity assessment scheme (CAS)
assesses QTSP/QTS
Design, testing, pre-production
Documentation
(Preparation of provision)
eIDAS conformity assessment report (CAR)
Notified TLSO
Compliance verification
Grant/ Withdraw Qualified status
Trusted List update

In addition to the initial conformity assessment as a prerequisite to the grant of a qualified status and hence to the provision of QTS, a QTSP/QTS must undertake at least every two years an assessment to confirm the QTSP/QTS continue to meet the requirements of the eIDAS Regulation (see Art. 20.1 of eIDAS). Furthermore, the competent SB *may at any time audit or request a conformity assessment body to perform a conformity assessment of the QTSPs, at the expense of those trust service providers, to confirm that they and the QTSs provided by them fulfil the requirements laid down in the eIDAS Regulation* (see Art. 20.2 of eIDAS). All those initial, ad hoc, and regular conformity assessments follow the same process described and illustrated above.

1.1.2 The eIDAS conformity assessment framework

The eIDAS Regulation requires the CAB to be accredited[1]:

- In accordance with 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.

However, the eIDAS Regulation does not place any further requirement neither for the NAB accrediting CABs, nor for the CAB assessing QTSP/QTS, nor for QTSP/QTS based on which the CABs should evaluate the conformity with the functional requirements set out in the eIDAS Regulation[2].

The European cooperation for Accreditation[3] (EA) is the body recognised under Regulation (EC) No 765/2008 to manage a peer evaluation system across NABs from the EU Member States and other European countries. EA has adopted the recommendation[4] to use an eIDAS accreditation scheme based on the [ISO/IEC 17065] accreditation framework, supplemented by

[1] Cf. Art.3(18), Art.20(1), Art.21(1).
[2] See ENISA report "*Towards a harmonised conformity assessment scheme for QTSP/QTS*" [ENISA - CAS] for discussions on further improvements in the harmonisation of eIDAS conformity assessments.
[3] http://www.european-accreditation.org/
[4] 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

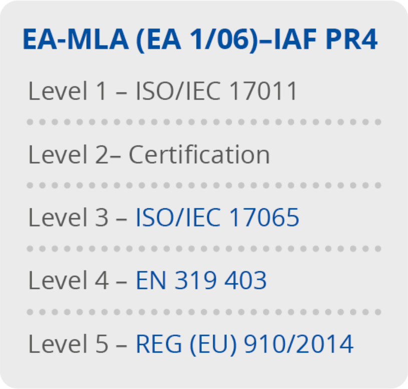
[ETSI EN 319 403][5], as one possible route for CABs to assess conformity with relevant requirements of the eIDAS Regulation.

The eIDAS accreditation scheme recommended by the EA, and illustrated in Figure 2 below, requires:

- The accreditation of the CAB to be 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.

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

Figure 2. eIDAS accreditation scheme recommended by EA



EA-MLA (EA 1/06)–IAF PR4

Level 1 – ISO/IEC 17011

Level 2– Certification

Level 3 – ISO/IEC 17065

Level 4 – EN 319 403

Level 5 – REG (EU) 910/2014

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. As a consequence, it is important that the certification scheme operated by the CAB (see clause 7.1.1 of ISO/IEC 17065) is well constructed and covers all relevant aspects of the eIDAS Regulation[6]. This

[5] ETSI [EN 319 403-1] has been adopted on 15 June 2020 as a new version of ETSI EN 319 403 (v2.2.2 in its latest version). The date of withdrawal of any conflicting National Standard is set to 31 March 2021. However, EN 319 403 has not been withdrawn and can still be referenced for use. At the date of publication of this report, the EA did not update its EA-GA Resolution 2014 (34) 22 (and Document EAGA(14)31) to switch from ETSI 319 403 to ETSI 319 403-1. As a result, the current situation is that the majority of eIDAS accredited CABs are still accredited and performing eIDAS audits under the old version of this ETSI standard. EA is encouraged to update its resolution and recommendation accordingly, NABs are encouraged to update their eIDAS accreditation schemes and the eIDAS accredited CABs are encouraged to abide by ETSI EN 319 403-1 in replacement of ETSI EN 319 403 when conducting eIDAS audits of QTSP/QTS. In the report, unless a precise version is pointed to, the notation “ETSI EN 319 403(-1)” will be used to refer to the applicable version of the standard.

[6] To this extent, eIDAS accredited CABs should comply with [ETSI TS 119 403-3], which specifies requirements on conformity assessment schemes and conformity assessment reports, including their content, for CABs assessing

scheme actually needs to be part of the NAB evaluation when accrediting CABs in the context of eIDAS. These certification schemes should be made publicly available and their eligibility and suitability under eIDAS be evaluated by SB when submitted resulting CARs by QTSPs.

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[7].

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 remain voluntary for QTSPs: their use remains optional.

1.2 PURPOSE AND STRUCTURE OF THIS DOCUMENT

This document provides an overview of the conformity assessment framework for (prospective) QTSPs in the context of the eIDAS Regulation, i.e. aiming to confirm that the assessed QTSP/QTS fulfil the requirements of this Regulation.

It discusses the typical process flow and the methodology used to perform such conformity assessments. For each phase of the assessment, guidance is provided to QTSPs for the purpose of preparing and undertaking the conformity assessment, as required by the eIDAS Regulation, in the best possible conditions. Section 2 presents an overview of the overall process flow of a conformity assessment. Section 3 stresses the importance of a dialogue with the competent SB. The next sections provide QTSP with specific guidance for each phase of the assessment: preparation (Section 4), conduction (Section 5), certification (Section 6), surveillance and renewal (Section 7). Frequently asked questions are provided in Annex A.

1.3 TARGET AUDIENCE

The document targets QTSPs, and TSPs without qualified status which intend to start providing QTS. Other stakeholders such as EU MS SBs, NABs, and CABs.

***Disclaimer**: To help (Q)TSPs with further guidance and illustration on these policies, procedures, and processes, the present document refers to ETSI and ISO/IEC standards. E.g. ETSI standards regarding trust services were specifically written with the purpose to help TSP to conform to eIDAS; they are designed to provide tailored security requirements for the different trust services components, based on best practices or more general standards.*

However, with regard to the technological neutrality of the eIDAS requirements, it is worth noting that:

- *Different approaches based on different technologies than the ones exposed in the present document can lead to eIDAS compliance;*
- *Compliance against these standards (or other standards) is not mandatory to achieve compliance against eIDAS requirements.*

Compliance against standards does not automatically imply conformance to eIDAS requirements. Although these standards may be seen as best practices, there is no automatic presumption of compliance to eIDAS when meeting the said standards.

QTSP/QTS against eIDAS. The EA eIDAS accreditation framework depicted in Figure 2 (level 4) should be extended to include this ETSI standard.

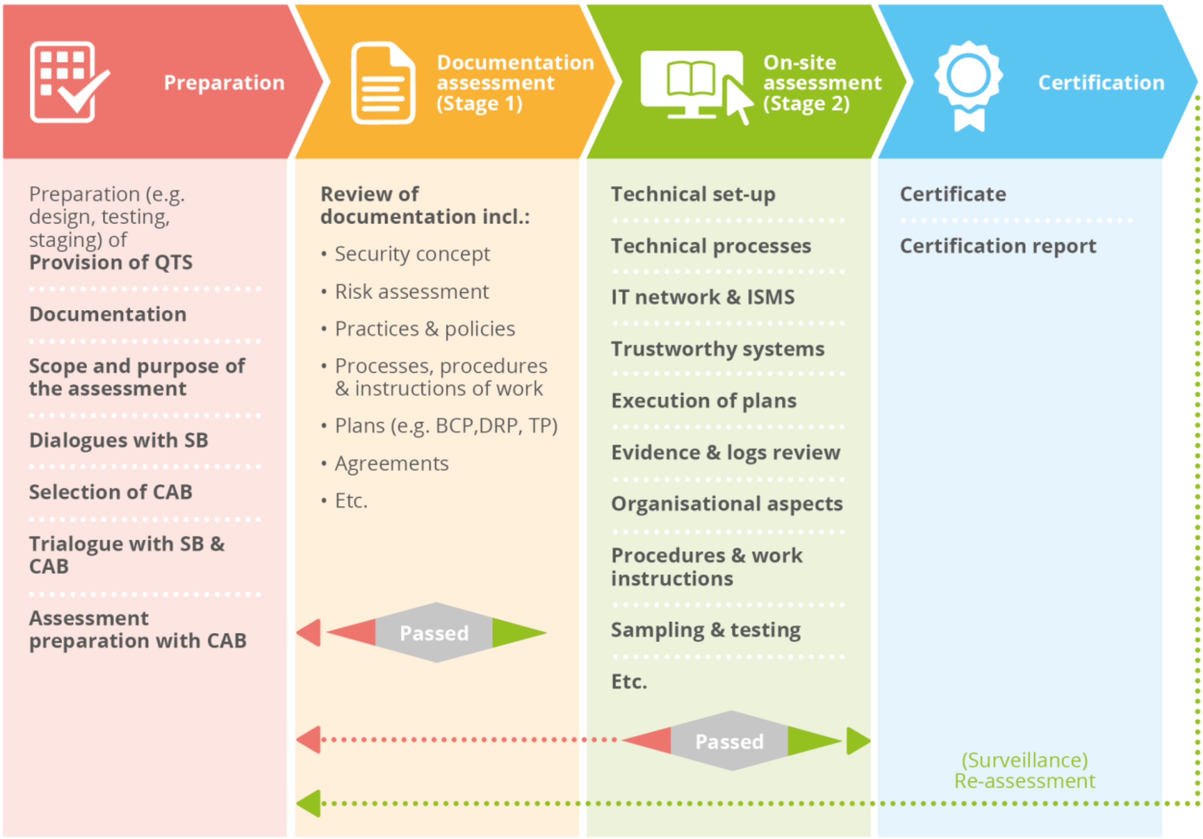
[7] Technical standards may however useful for QTSP/QTS, respectively for CABs, and facilitate the demonstration, respectively the evaluation, that they meet the applicable requirements of the eIDAS Regulation. The ENISA guidelines "*Recommendations for QTSPs based on standards (2020)*" [ENISA - QTSP standards] provide recommendations to help qualified trust service providers and auditors understanding the expected mapping between these requirements/obligations and reference numbers of standards, as well as practical recommendations for their usage

2. TYPICAL CONFORMITY ASSESSMENT PROCESS FLOW

2.1 OVERVIEW

As part of the EA recommended framework (see previous section), ETSI [EN 319 403-1] supplements [ISO/IEC 17065] to provide additional dedicated requirements for CABs performing certification of QTSP/QTS towards criteria against which they claim conformance[8]. This section presents the general approach for CABs to conduct assessments in line with [EN 319 403-1].

Figure 3. Typical conformity assessment (certification) process flow [9]



Following an appropriate preparation, [EN 319 403-1] requires the assessment to include at least two stages:

- A **documentation assessment** (Stage 1) to review the design and the documentation regarding the (Q)TSP and the (Q)TS it provides or intend to provide.

[8] In the context of an assessment of the conformity of QTSP/QTS against eIDAS, these criteria shall be the requirements of the eIDAS Regulation itself.

[9] The illustrated "Preparation" phase is under the responsibility of the QTSP; other phases fall under the responsibility of the CAB.

- An **on-site assessment** (Stage 2), which aims to validate the findings of the previous stage and to complete the assessment of the QTSP/QTS services against the targeted assessment criteria, with support of on-site visits.

At the end of stage 2, the CAB will issue the QTSP with a CAR containing all the results of the assessment. When these results include any non-conformity to the targeted criteria, no certification of conformity will be issued and the (Q)TSP will be requested to produce and execute a plan of corrective actions.

It is only in the absence of any non-conformity with regards to the targeted criteria (potentially subject to the review and assessment of the correct execution of a plan of corrective actions to solve non-conformities identified in a previous version of the CAR) that the CAR will be complemented by a formal certification decision confirming that the assessed QTSP/QTS meet (i.e. are conformant with) the targeted assessment criteria.

> Note: A key update of ETSI [EN 319 403-1] compared to [EN 319 403] is the removal of the possibility for a CAB to issue a positive-like (i.e. "passed") certification decision while there are still pending non-conformities with the target criteria against which the TSP and the TS it provides are assessed (cf. update of clause 7.6 of the referenced standards).
>
> In the context of QTSP/QTS, Art.20(1) of the eIDAS Regulation is making explicit that the purpose of the audit is "*to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation*". This does not leave any room for any non-conformity with the requirements of the Regulation.
>
> ETSI [EN 319 403-1] allows the CAB to issue a certification report identifying non-conformities indicating their severity based on the substantial security impact and/or substantial impact on the ability of the QTSP/QTS to meet the eIDAS requirements. However, in this case, the CAB shall not issue a "certified" decision attesting that the audited trust service fulfils the criteria and is certified conformant. For continuing the process, the QTSP will be required by the CAB to implement a corrective action plan before the CAB could assess and confirm the QTSP/QTS are conformant with the eIDAS requirements.
>
> For a prospective QTSP, in the event of a CAR and certification decision being issued with pending non-conformities to be solved within a determined period, the competent SB, to which such CAR would be submitted, shall require the prospective QTSP to solve all non-conformities and have the CAB to evaluate and confirm their correct implementation before considering the CAR as eligible under Art.21.1.
>
> In the context of an existing QTSP and regular 2-yearly audits, the non-conformities identified in an eIDAS CAR (which must be submitted to the SB within the period of three working days from reception by the QTSP) will need to be solved, with the (CAB and/or QTSP) indicated deadline by which they should be solved being confirmed or adjusted by the SB, their resolution confirmed by the CAB in the resulting CAR and, when this is the case, in a positive certification decision, before the SB may confirm the grant of the qualified status.

In the context of the eIDAS Regulation, it should be noted that a certification of conformity of the assessed QTSP/QTS against the eIDAS requirements does not automatically mean that the QTSP/QTS will be granted a qualified status[10]. The final decision on the grant of such a

[10] It is worth noting that the certification of a QTSP/QTS against any standard is out of scope of the eIDAS Regulation. Compliance against any standard is not required by eIDAS, does not automatically imply conformance to eIDAS requirements, and gives no automatic presumption of compliance to eIDAS when met. Cf. section 1.1.2 of the present document.

qualified status belongs to the competent SB after it has verified that the QTSP/QTS comply with the requirements laid down in this Regulation[11]. The notification to the SB of a CAR confirming that the assessed QTSP/QTS meets the eIDAS requirements is a necessary condition but it might not be a sufficient one. The grant decision will be based on the CAR and on any additional information/ evidence required from the (prospective) QTSP necessary to verify that the eIDAS requirements are met.

2.2 PREPARATION OF THE ASSESSMENT

The preparation of an assessment does not start with the preparatory meeting with the selected CAB. Like for any type of service, the provision of QTS may require a heavy preparatory phase. This includes the design, testing and staging of the provision infrastructure and associated processes, often requiring several iterations before being ready for production.

A key aspect of this preparatory phase, as well as for the entire life cycle of the QTS provision, lays in the documentation. The documentation may often be considered as the main asset of the QTSP, more than the QTSP private keys and other trustworthy systems or devices. It is the basis on which the trustworthiness and compliance of the QTS provision, and of the associated private key(s), can be demonstrated and evidenced, not only to the CAB but to the supervisory body, the customers and the relying parties. Typical structure and list of contents for such a documentation is further discussed in section 4.2.

An early dialogue with the SB is strongly recommended e.g. to clarify the scope of the assessment, the SB requirements on the assessment and in particular on the CAR structure and CAR content specifications, as well as on the CAB itself (e.g. accreditation scheme, certification scheme).

Before starting the audit and actually before the appropriate CAB is selected and contracted, the CAB and the (prospective) QTSP will define and agree on the plan and scope of the audit. This will include notably to clarify:

- The methodology of the audit;
- The timing and effort required for the audit;
- The exact locations/sites where the various assessment stages will take place;
- The testing and sampling policy;
- The certification statement on the certificate and CAR;
- The structure of the CAR;
- The surveillance program, if any.

It is recommended for the agreed plan and scope of the audit, in particular the above listed points, to be validated by the SB (e.g. in a (prospective) QTSP – SB – CAB trialogue approach).

2.3 CONDUCTION OF THE ASSESSMENT

2.3.1 Stage 1 – Documentation assessment

During the first stage of the audit, the CAB will develop its understanding of the structure and scope of the QTS provided by the QTSP, before defining an appropriate planning for stage 2 of the assessment.

On top of the documentation provided by the QTSP at the start of the assessment[12], the CAB can, at any time, request additional information from the QTSP. This may include evidence

[11] To this extent, the SB may contest CAR's reported recommendation(s) and request improvements so that no non-conformities exist.
[12] Refer to section 4 for details on the documentation to be provided.

records, description of the design of QTS, work instructions associated to specific procedures, samples of QTS outputs, etc.

At the end of stage 1, the CAB will provide the QTSP with a first findings report. This report contains the results of the design and documentation review and highlights the areas of concerns along with recommendations. Although minor issues may remain open and solved during the next stage, identified issues (including missing pieces of documentation) need to be resolved before the start of stage 2.

Stage 1 and stage 2 should not be carried out in a row, but rather allow time for handling the findings of the stage 1 audit. In determining the interval between stage 1 and stage 2 audits, [EN 319 403-1] requires to take into consideration the needs of the QTSP to resolve areas of concern identified during the stage 1 audit; this may require the CAB to adjust arrangements for stage 2.

Next to this stage 1 report, the CAB will also share an assessment plan for stage 2 with the QTSP and may request additional information or records, when necessary to the conduction of stage 2. Planned activities can include scheduled and unscheduled on-site visits, interviews with personnel, collection and inspection of facilities, of records, and of evidences, testing, etc. In function of stage 1 results, the sampling methodology, taking into account the size of the service provision and the number of involved facilities and sites, will be finalised. Stage 2 assessment plan must be consistent with the findings identified during stage 1. The plan will be sent to the QTSP, together with stage 1 report, after the closure of the stage 1.

2.3.2 Stage 2 – On-site assessment

Once all stage 1 activities are completed and main issues or areas of concerns are resolved by the QTSP, stage 2 can be started.

This stage takes place on site, at the premises of the QTSP and of all or parts of its (sub-)contractors operating (key) components of its QTS provision.

While stage 1 could be seen as a verification that the required documentation is present and fits the purpose of demonstrating the conformity of the QTSP/QTS to eIDAS, the purpose of stage 2 is to evaluate the demonstration by the QTSP/QTS that they comply with their own policies and procedures, and particularly that they meet the target assessment requirements, i.e. the eIDAS requirements applicable to QTSP/QTS in the case of an eIDAS assessment. To this latter extent, as the requirements of the eIDAS Regulation on QTSP/QTS are functional requirements, it is key that the certification scheme operated by the CAB is well constructed and covers as many evaluation criteria, leveraging on recognised basis such as standards, as needed to assess the conformance of the conformity with the Regulation.

To perform such an evaluation, the CAB will collect evidences, e.g. records and/or logs of every action and operation of the provision of QTS by the QTSP, including those related to:

- The processes, procedures and work instructions related to the provision of QTS;
- The trustworthy systems and products used;
- The information security measures implemented to protect the QTS provision;
- The physical security of relevant sites.

The stage 2 will result in the production by the CAB of a CAR providing the results of the evaluation and assessment checks of the conformity of the assessed QTSP/QTS with the targeted assessment criteria. The report will identify and detail all non-conformities, supported by objective evidence when applicable and a reference to the requirement that is not fulfilled.

The CAR may also include recommendations for improvements, not necessarily related to non-conformities, which aim to improve, in the views of the CAB, the way the QTSP/QTS may fulfil and demonstrate the fulfilment of the assessment criteria.

2.3.3 Non-conformities and recommendations for improvements

The identification of any non-conformity with the targeted assessment criteria will prevent the CAB to issue a positive certification decision. A certificate of conformity may only be issued when all actions aiming to correct the reported non-conformities have been conducted and these non-conformities have been solved.

If the (Q)TSP expresses interest in continuing the evaluation process, it needs to provide a plan of corrective actions to the CAB aiming to resolve the identified findings and non-conformities within a given period of time. The CAB will validate the plan and verify that the non-conformities have been corrected.

A plan of recommended improvements may be established, validated, executed, and verified in parallel with the plan of corrective actions.

2.4 CERTIFICATION

It is only when the CAR confirms the absence of any non-conformity to the targeted assessment requirements, taking into consideration the implementation and the verification of the correct implementation of potential corrective actions, that the CAB may issue a positive certification decision and a corresponding certificate of conformity.

In the framework of [ISO/IEC 17065], the CAR and the certification decision (leading to the conformity attestation in the form of a conformity certificate) are two clearly distinct steps in the certification process. The certification decision "certified" (cf. clause 7.6 of [EN 319 403-1]) aimed to mean, in the context of an eIDAS audit, that the assessed QTSP/QTS is confirmed to meet the applicable requirements of the eIDAS Regulation, may only be taken when the absence of any non-conformity to these requirements is confirmed

2.5 SURVEILLANCE AND RE-ASSESSMENT

In the context of the eIDAS Regulation, QTSP/QTS shall be re-assessed (full re-assessment audit) at least every 24 months.

The eIDAS Regulation does not place any requirement on intermediary surveillance assessments. However, when the eIDAS conformity assessment is conducted under the framework of ISO/IEC 17065 and in particular in line with ETSI EN 319 403(-1), in addition to the 2-yearly full re-assessment, the CAB shall define a programme of periodic surveillance assessments that includes on-site audits to verify that the certified QTSP/QTS continue to comply with the assessment criteria (e.g. the eIDAS requirements). It is recommended, and sometimes required by some SBs, that at least one surveillance audit per year is performed in between full assessment audits.

Surveillance assessments do not need to be full system assessments but include:

- An evaluation of effectiveness and sustainability of the corrective action plan(s) and of the resolution of the related non-conformities identified during previous CAR and solved at the occasion of previous assessments;
- A review of actions taken on suggestions for improvement that were identified in the previous assessment(s), not defined as non-conformities, and whose implementation is pending;
- A review of the multi-site sampling strategy, if sampling was applied in the previous assessment;

- A review of any changes in the documentation and QTSP operation to provide its QTS, including any impact on the termination plan;
- A review of internal audits and security management systems in place;
- A review of the treatment of complaints;
- A review of the use of marks and/or any other reference to conformity assessment;
- A review of any public QTSP's statements with respect to its operations (e.g. promotional material, website, use of EU trust mark for QTS).
- A review of a sample of records relating to the operation of QTSP/QTS over the historical period since the previous assessment.
- A review of incident detection, reporting and handling.

Surveillance assessment report findings may have an impact on the certification decision when non-conformities are identified.

Major changes in the QTSP documentation, in its operation and more generally in the provision of its assessed and certified QTS may result in the need for a full re-assessment prior to the 24 months period. The CAB will establish a procedure with the QTSP to deal with changes affecting certification. This includes notification of the change and determination of appropriate conformity assessment activities to assess that the conditions for certification are still met. Notification and decision need to be performed before implementation of the measures.

It is worth noting that ad hoc audits conducted by the QTSP’s competent SB, once a QTSP has being granted a qualified status, or conducted at the SB’s request by a CAB, which may be selected by the SB and be different than the CAB contracted by the QTSP, are, per nature, not scheduled in the surveillance program established between the CAB and its client QTSP. These ad hoc audits, pursuant to Art.20.2 of eIDAS, may be decided by the SB at its own discretion, subject to the principles of good administration.

3. DIALOGUE WITH SUPERVISORY BODY

In the context of the eIDAS Regulation, the SB is the entity having final decision on the grant of a qualified status after it has verified that the QTSP/QTS comply with the requirements laid down in the Regulation. The grant decision will be based on the CAR and on any additional information/evidence required by the SB necessary to such a verification.

To this extent, a key recommendation is to engage as soon as possible a dialogue with the competent SB. This dialogue is key throughout the entire life cycle of the QTS provision by the QTSP, from its genesis until after the QTS termination, and in particular with regards to the initial, regular, and ad hoc assessments for confirming compliance with the applicable eIDAS requirements. It is often the case that SBs do have specific requirements, e.g. on the scheme used for accrediting the CAB and its assessors, on the assessment methodology, or on the structure and content of the CAR.The topics for the dialogue with the SB on the eIDAS conformity assessment include.

Table 1: Dialogue with the SB on the eIDAS conformity assessment

ASSESSMENT PREPARATION	□ Information on eIDAS Art.21.1 and/or Art.20 notification procedure and required documentation; **Before CAB selection** □ Validation of the eligibility and suitability criteria for the selection of the CAB; □ Information on SB's requirements, if any, on: □ The scope, purpose and methodology of the QTS assessment, including: □ The timing and effort required for the audit; □ The testing and sampling policy; □ Composite certification and handling of composite audits; □ The scope, structure and (table of) content of the CAR; □ The surveillance program; □ SB's involvement in assessment stages (e.g. observation); **After CAB selection** (e.g. as a (Q)TSP, SB, and CAB trialogue) □ Inform about selected CAB and team of assessors; □ Validation of the scope, purpose and methodology of the QTS assessment, including planned audit timing and efforts, as well as testing and sampling policy; □ Inform about exact locations/sites where the various assessment stages will occur; □ Validation of the scope, structure and (table of) content of the CAR; □ Validation of the planned surveillance program; □ Inform on the exact dates of the planned assessment phases.
ASSESSMENT CONDUCTION	□ For QTS/QTS, notification of any non-conformities, hence impacting certification decision and grant of qualified status.
ASSESSMENT COMPLETED	□ Notification of CAR (together with the relevant assessed documents, e.g. assessed up-to-date termination plan, incident management/notification plan[13]). □ Validation of the surveillance program.

[13] Refer to section 5.3 and ETSI TS 119 403-3 for further details.

4. PREPARATION TO ASSESSMENT

4.1 TARGET OF ASSESSMENT

One of the most important preparatory points to a QTSP/QTS assessment, if not the most important, is to clearly define the scope and target of the assessment.

4.1.1 Service components

The QTSP is the person (natural or legal) having the final responsibility and liability to provide a QTS, in line with the requirements of the eIDAS Regulation. In many cases, a QTSP relies on one or more (sub-)contractors or partners to operate one or more components of the QTS it provides. A well-known example is the operation of (local) registration authority facilities as a component part of the provision of (qualified) electronic certificates. Furthermore, the provision of (qualified) electronic certificates as a QTS may be divided in many more service components such as the registration, the certificate generation (or factory), the dissemination, the revocation management, the certificate validity (or revocation) status, the subject (cryptographic) device provision[14]. In extreme cases, a QTSP may limit its operational role to the legal liability, governance and responsibility of the QTS provision while delegating or sub-contracting the operation of all service components to contracted parties[15].

In the context of the eIDAS Regulation, the provision of QTS is the sum of the provision of all its service components. Hence the assessments required under the eIDAS Regulation need to cover the provision of the QTS as a whole, including each and every one of its components.

It may happen that, prior to the eIDAS conformity assessment of the whole QTS they are part of, some of the QTS components have been individually assessed against specific set of requirements independently of the eIDAS Regulation but in a way that the resulting assessment reports may serve the demonstration that the whole QTS meet the eIDAS requirements. The specific set of requirements may be private sector specifications, technical standards or even a sub-set of the relevant eIDAS requirements. For example, a network of registration authorities are assessed being conformant with (e)KYC requirements as per the Banking sector.

As a general approach[16], existing certification attestations, whether applicable to the provision of a QTS as a whole or to one or more of its service components, may be taken into account by the CAB selected to conduct a conformity assessment of a QTSP/QTS. But, the eIDAS assessment conducted by the CAB must verify the applicability of such prior certifications in the context of the eIDAS assessment and remains responsible and liable for the certification decision confirming the conformity of the assessed QTSP/QTS, as a whole, with the eIDAS requirements.

However, composite certification and handling of composite audits, where components (and/or processes) of a QTS are audited separately by different CABs without having to repeat a full

[14] See clause 4.4 of ETSI EN 319 411-1 for a discussion on the breakdown of the provision of certification services into service components.
[15] In such cases, however, it is expected that the governance and key related topics must still be performed by the QTSP legal entity itself, e.g. risk management, involvement/approval by management, asset management. Showing control may be difficult without ownership on these.
[16] Cf. clauses 1, 7.4.1.0 and 7.4.4.4.(d) of ETSI EN 319 403-1.

assessment of all components, might not be recognised or accepted by the competent SB or under applicable national regulations, or being subject to specific requirements.

QTSPs intending to undertake or willing to benefit from separate audits/certifications from different CABs should verify that:

- □ The service component certification scheme(s) used
  - □ were designed to allow 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;
  - □ resulted in certification attestation letters and CAR that clearly identify such schemes, the scope of the certification and the conditions for the certification to be valid, including those related to interfacing other QTS service components;
- □ Such practices are recognised by the competent SB and meet the requirements the SB may have on these practices;
- □ Such QTS component certifications are recognised by the selected CAB and requirements it may have on handling them;
- □ CAB's rules for accepting and handling existing QTS component certifications are clearly established in CAB's CAS on assessing QTSP/QTS against eIDAS, including checks:
  - □ on the scope and relevance of the QTS component certification and that the certification conditions are met;
  - □ that the [eIDAS] requirements of the service component including its security are met, and checks that the trust service use of the component interface meets the requirements as specified by the service component provider (as required in clause 7.4.4.4 point (d) of ETSI EN 319 403-1) and as specified in the component certification conditions;
  - □ that the time between audits of a trust service component is no longer than the time between assessments of the QTS using the component (see clause 7.9 of EN 319 403-1);
  - □ that the way earlier assessments and certifications are taken into account will be documented in the CAR.

See ENISA report "*Towards a harmonised Conformity Assessment Scheme for QTSP/QTS*" [ENISA - CAS] for further considerations on the harmonisation of scheme rules regarding QTS composite certifications and their handling in assessing QTSP/QTS against the applicable requirements of eIDAS.

4.1.2 eIDAS scoping of the assessment

In the context of the eIDAS Regulation, all assessments of QTSP/QTS must confirm that the QTSP/QTS fulfil the requirements laid down in this Regulation. The CAR and the conformity assessment certificate or attestation letter must explicitly bear a clear statement confirming - if such is the case - that the assessed QTSP/QTS meet all the applicable requirements of the eIDAS Regulation[17].

As reminded in section 1.1 of the present document, the normative document (or target criteria) against which the CAR and the corresponding certificate or attestation letter must confirm the conformance of the assessed QTSP/QTS is not a technical standard but the QTSP/QTS applicable requirements from the eIDAS Regulation itself. QTSPs are free to implement any

[17] It is worth stressing again that, as the requirements of the eIDAS Regulation on QTSP/QTS are functional requirements, it is key that the certification scheme operated by the CAB is well constructed and covers as many evaluation criteria, leveraging on recognised basis such as standards, as needed to assess the conformance of the conformity with the Regulation.

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. A certification against any technical standard would not meet the eIDAS conformity assessment requirements and would not even create a legal presumption of compliance with any requirement of the eIDAS Regulation[18]. To this extent, the QTSP is recommended to:

- □ require the selected CAB to conduct the QTSP/QTS eIDAS assessment and in particular produce the resulting CAR in conformance with ETSI TS 119 403-3 [19].

4.1.3 Multipurpose assessment

In many cases the provision of QTS by a QTSP may need to comply with additional requirements than those laid down in the eIDAS Regulation. As an example, QTSPs issuing QWACs need to comply with CAB/Browser Forum requirements and additional requirements from browser and application vendors in order for these QWACs to be recognised in said browsers or applications. Another example could imply a sectorial or industry corporation requiring the provision of QTS to meet specific technical standards.

It is also common that a QTSP is willing to mutualise its efforts and resources, as well as the ones form the CAB, to use the same audit process and period to assess several types of QTS it may provide or intend to provide.

Considering the costs, time and personnel resources required to be invested in passing a conformity assessment, it is understandable that QTSPs will seek to mutualise as much as possible the conformity assessment efforts in order to benefit from as many confirmations as possible that they meet different sets of target assessment criteria.

As a general approach, without prejudice to the possibility to combine a sub-set of assessment tasks performed by the CAB, it is strongly recommended that multipurpose or combined assessments result in as many dedicated CARs and attestation letters as there are different sets of target assessment criteria.

4.2 DOCUMENTATION

It is essential for QTSPs to make sure the appropriate documents supporting the provision of its QTS(s), including plans, policies and procedures, are defined and continuously updated following the changes in the QTS provision, from its genesis to its termination. This is key not only for the QTSP to ensure the QTS provision is according to its expectations & plans but also in line with customer and relying parties’ expectations. It is also crucial to assist in the demonstration that QTSP/QTS meet specific requirements, including those for which an evaluation of such conformity is required, e.g. the applicable eIDAS requirements.

As part of its audit activities, the CAB will request specific documentation supporting the implementation of the assessed QTSP/QTS. As little as possible documentation should be created on purpose for the sake of the assessment[20], most if not all parts of the documentation should already exist, be approved and in use when QTS is provided. The assessment aims to verify that this is the case and the provided QTS is implemented in accordance with the QTSP documentation and with the target assessment criteria. An index structuring the access to the

[18] This might however be the case at national level where a national legislation or administrative decrees would introduce such a presumption of compliance for those QTSPs that comply to nationally defined specifications, usually defined by leveraging on CEN/CENELEC and ETSI standards and/or profiling them, When not associated to a formal presumption of compliance, these national specifications may be presented as key instruments to facilitate the evaluation by CABs of the conformity of QTSPs/QTSs with the eIDAS requirements. Refer to [ENISA - CAS] for further considerations on the harmonisation of scheme rules regarding the assessment of the conformity of QTSP/QTS against the applicable requirements of eIDAS.

[19] Some EU MS SBs do require eIDAS CARs to be structured in compliance with ETSI TS 119 403-3.

[20] To the notable exception of a QTSP self-assessment of the QTSP/QTS conformance with the applicable eIDAS requirements.

documentation is recommended to be maintained and provided to the CAB together with the documentation.

The documentation typically includes, as illustrated in Table 1, documents describing the company and the way it has organised the governance of the provision of QTS, agreements with sub-contractors/partners, customers, and relying parties, documents describing how it complies with regulations and/or standards, documents stating the policies and practices used for the provision of QTS, and a long list of documents related to the technical implementation and management of such QTS provision, including relevant plans, policies, processes, procedures, work instructions as well as records and/or logs evidencing their implementation.

Plans are high-level statements that aim at providing a clear understanding of the long-term objectives defined by the Trust Service Providers throughout the organization and are periodically reviewed and updated by the management. Policies are principles, rules or guidelines established and adopted by Trust Service Providers to influence or determine the way of proceeding in specific cases or areas, in line with the established plans.

In order to concretely implement the provision of QTS in line with the plans and policies, QTSPs need to define processes, procedures and work instructions supporting such implementation, where:

- An overall process (hierarchy) description shows the chain of activities that use resources to transform inputs into outputs (cf. ISO 9001). In case of QTS provision, it means the chain of activities aimed to achieve the goals of the plan in line with the associated policy(ies).
- Existing procedures describe the specified way to carry out the activities of the process, and
- Existing "work instructions" describe in detail how an activity within a process (or procedure) is performed. Going down to work instructions is key as they allow to reduce risk and errors and save time. This is typically the goal of ISO 9001 certification.

The creation and update of the existing plans, policies, processes, procedures, and work instruction should be reviewed and receive the approval, before their publication and/or activation, from the management of the QTSP, which is usually operationalised into a QTSP governance body responsible for the provision of QTS (usually referred to as the PMA – Policy/PKI Management Authority). The same body should be responsible for the correct execution of these processes, procedures, and work instructions in conformance with plans and policies and review audit results evaluating such conformance as well as conformance with specific target assessment criteria (e.g. standards, eIDAS requirements).

A recurrent issue in the relationship between the QTSP and the CAB (and team of assessors) is the confidentiality of sensitive information, despite the signature of appropriate non-disclosure agreements. The key principle is that, if the CAB concludes that access to an information is required to demonstrate and warrant an effective audit, then the QTSP needs to accept and arrange appropriate access to this confidential or sensitive information. If not, the conformity assessment may not take place.

The documentation referred to in Table 1, and further described in Annex B is the typical documentation:

- that the QTSP should establish and maintain in the context of the provision of its QTS(s), and
- that should be provided or made accessible to the CAB as from stage 1 and reviewed by the CAB during the assessment.

Table 2: QTSP/QTS typical documentation

QTSP company documentation

- □ Legal statutes / Memorandum and Articles of Association
- □ Extracts of official registers (e.g. evidence of official name and, when applicable, of registration number)
- □ Company blue prints (e.g. company shareholders, company organigram)
- □ Information on the QTSP's economic resources
    - □ Audited financial statement (e.g. for the last 3 years)
    - □ Evidence of liability insurance and/or of capital adequacy for the provision of QTS

      Note: The enclosed information must be able to show sufficient economic resources to be able to run a business in accordance with the requirements laid down in eIDAS Regulation and national laws for QTSP/QTS
- □ Organisation of the QTS management by the QTSP
    - □ PMA (Policy/PKI Management Authority) documentation, including composition, internal rules of procedures, meeting and decision records
    - □ QTSP/QTS organisation structure (overview and description of functional roles and responsibilities together with their allocation to identified personnel/staff, either internal or external to the QTSP) including the identification of the external contractors/partners involved in the provision of QTS components, their roles and responsibilities
- □ Contractual agreements
    - □ Agreements with (sub-)contractors and/or partners for the provision of QTS, incl. service components
    - □ General terms and conditions (towards customers and relying parties)
    - □ general template(s) and signed/approved version of the customer agreements (e.g. contracts)

eIDAS conformity *(and other regulations, when applicable)*

- □ eIDAS conformity self-assessment (check-list)
- □ Previous certificates of conformity of the QTSP/QTS or of components of the QTS to the eIDAS requirements
- □ Other regulations: when applicable, attestations of conformity with other national, regional, or international regulations, whether public (e.g. legislation based) or private (e.g. Industry based).

Compliance with standards

- □ List of standards to which operations are audited, evaluated, certified or assessed to be compliant and details about the associated certificates of conformity, and the underlying audit, evaluation, certification or assessment schemes (e.g. certification against ISO/IEC 27001 and/or ISO/IEC 27701, certification against relevant ETSI ESI standards)
- □ List of additional standards with which operations are claimed to be compliant (no external attestation)
- □ A cross-reference document linking the individual eIDAS requirements with the individual controls of the standards relevant to support the demonstration of eIDAS conformity.

QTS policy and practices statements

- □ Declaration of practices for the provision of QTS (i.e. CPS or Trust Service Practices Statement)
- □ Trust services policies (e.g. Certificate Policies - CP, time stamping policies, etc.)

QTSP/QTS technical documentation

- □ QTS provisioning overview: A general overview of the scope of the (Q)TS provided, of the technical and organisational blueprints, of the used locations/sites, of the (Q)TS size, of the service components and of the associated (sub-)contractors
- □ Trust service detailed architecture, e.g.:
    - □ High-level and Low-level design overview
    - □ PKI hierarchy along with the indication of the supported trust service policies
- □ Detailed technical documentation (e.g. detailed and complete description of the technical, physical and logical infrastructure)

Plans, policies, processes, procedures, work instructions and evidences for the provision of QTS						
Areas	**Plans**	**Policies**	**Processes**	**Procedures**	**Work instructions**	**Evidences, records, logs**
QTS Infrastructure Management (incl. change management)	□	□	□	□	□	□
QTS provision operations (e.g. on a component per component basis)	□[21]	□[22]	□	□	□	□
Data privacy and GDPR	□	□	□	□	□	□
Security Including:						
Asset inventory	□	□	□	□	□	□
Risk Management	□	□	□	□	□	□
Information Security Management	□	□	□	□	□	□
Physical Security	□	□	□	□	□	□
Access control Management	□	□	□	□	□	□
Incident						
Incident management	□	□	□	□	□	□
Incident notification	□	□	□	□	□	□
Communication	□	□	□	□	□	□
Business continuity	□	□	□	□	□	□
Contingency	□	□	□	□	□	□
Disaster recovery	□	□	□	□	□	□
Termination	□	□	□	□	□	□
Legal enforcement	□	□	-	-	-	□
(Trusted) Personnel						
(Trusted) Personnel recruitment	□	□	□	□	□	□
(Trusted) Personnel tasks allocation	□	□	□	□	□	□
(Trusted) Personnel training	□	□	□	□	□	□
Testing	□	□	□	□	□	□
Internal audit/quality monitoring	□	□	□	□	□	□
External audits (**including** resulting **CAR**s)	□	□	- from selected CAB(s) -			□
Recording and archival	□	□	□	□	□	□

[21] E.g. Declaration of practices for the provision of QTS (i.e. CPS or Trust Service Practices Statement).

[22] E.g. Applicable trust services policies (e.g. CP, time stamping policies, etc.)

In the context of the assessment of the conformity of a QTSP/QTS to the eIDAS requirements, a key document is the document reporting the self-assessment by the QTSP of such a conformance. This eIDAS self-assessment is not a requirement from the eIDAS Regulation but is a recommended instrument for the QTSP when preparing the design, the set-up and implementation of the QTS it intends to provide. This document should take the form of a check-list structured along the applicable requirements of the eIDAS Regulation (see CAR-4.2-16 of ETSI TS 119 403-3 for guidance), as it will also likely be used by the CAB to evaluate the demonstration of the QTSP that he and the QTS it provides or intend to provide meet the eIDAS requirements. While it is true that compliance with any standard will not guarantee a compliance with the eIDAS Regulation, standards and standardised check-lists may greatly support QTSP and facilitate their demonstration that they and the QTS they provide or intend to provide fulfil the applicable eIDAS requirements. See ENISA guidelines “*Recommendations for QTSPs based on standards (2020)*” [ENISA - QTSP standards] for further guidance on standards that can be used to support the demonstration of fulfilling the requirements of the eIDAS Regulation.

Depending on the type of QTS provided and on the scope and size of such a provision, the documentation can be significant both in terms of quantity and complexity. This documentation will be reviewed at the first stage of the conformity assessment and will serve as a basis for the on-site assessment performed during the stage 2.

4.3 SELECTION OF CAB

The eIDAS Regulation requires the CAB to be accredited by a NAB in the framework of Regulation (EC) No 765/2008 [Reg.765, 2008] and for the execution of a conformity assessment scheme suitable for confirming that, for a specific type of QTSP/QTS, a QTSP and the QTS it provides meet the applicable requirements of the eIDAS Regulation.

The following checks should be performed when selecting a CAB for the conduction of a QTSP/QTS assessment for their conformity against eIDAS.

Table 2: Checks when selecting a CAB for the conduction of a QTSP/QTS assessment

Selection of Cab

Requirement

- □ The CAB is accredited by a NAB in the framework of Regulation (EC) No 765/2008 [Reg.765, 2008] and for the execution of a conformity assessment scheme suitable for confirming that, for a specific type of QTS, a QTSP and the QTS it provides meet the applicable requirements of the eIDAS Regulation.

Recommendations

- □ The CAB should be listed on the EC compiled list of CABs accredited against the requirements of the eIDAS Regulation[23];
- □ The accreditation certificate should:
  - □ Either
    - □ be issued by a NAB that is a full member of the EA and a signatory of the MLA for the scope of product certification (i.e. ISO/IEC 17065),
    - □ confirm the accreditation scope of the CAB under the EA recommended eIDAS accreditation scheme, i.e.
      - □ under the ISO/IEC 17065 framework
      - □ supplemented by ETSI EN 319 403 (or its successor EN 319 403-1), and
      - □ for assessment of QTSP/QTS against the requirements of eIDAS; and
    - □ confirm the above scope of accreditation covers the specific type of QTS the QTSP is willing to assess conformance against the eIDAS Regulation[24].
  - □ Or be issued under another normative scheme provided such an alternative normative scheme has been recognised as equivalent.
- □ The accreditation certificate should identify the CAB’s eIDAS conformity assessment scheme.
- □ The CAB’s eIDAS conformity assessment scheme, preferably identified in the CAB eIDAS accreditation certificate, should:
  - □ be made publicly available and
  - □ provide detailed information on how the CAB shall conduct the assessment of a QTSP/QTS to confirm they meet the applicable eIDAS requirements.
- □ In case of multipurpose assessment, the QTSP should make sure, when a single CAB is selected, that:
  - □ the CAB is appropriately accredited for conduction of the assessment of the QTSP/QTS against each relevant set of the targeted assessment criteria[25];
  - □ the assessment will result in as many separate attestation letters (certificates) and CARs as required.

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

[24] A CAB may be accredited for assessing one or more, but not necessarily all of the nine types of QTS specified by the eIDAS Regulation.

[25] Audit for compliance against these ETSI standards (by a CAB qualified for audits against ETSI EN 319 411 standards series) is recognized by browsers for inclusion of QTSP’s certification authorities (CAs) in the root stores. Alternatively, demonstration of compliance via the WebTrust Program for CAs is another recognized path, hence a (Q)TSP intending to issue (or issuing) QWACs may decide to select a CAB that is both an eIDAS accredited CAB to assess the conformance of the QTSP/QTS with eIDAS and a licensed WebTrust practitioner for confirming compliance with CA/Browser Forum and Browser or Application Vendors requirements.
Another example would be a QTSP issuing qualified time stamps that decides to be certified against a specific (set of) standard(s) such as [EN 319 421] and [EN 319 422] in addition to its certification against eIDAS. In this latter case, the CAB must be accredited for conducting assessment against the eIDAS Regulation and for conducting assessment against the targeted standards.

4.4 ORGANISATIONAL ASPECTS

Ideally before contracting the CAB, and in any case before the start of the assessment, the QTSP and the CAB should agree on the scope and plan of the assessment, in particular:

- The eIDAS Regulation requirements applicable to the concerned QTSP/QTS to be the normative document and target assessment criteria, i.e. that the assessment will aim to confirm, when this is the case, that the assessed QTSP/QTS meet the applicable eIDAS requirements;
- The CAS and the structure of the CAR to meet ETSI TS 119 403-3;
- In case of a multi-purpose assessment, the assessment to result in as many CARs and certificates (attestation letters) as there are distinct target assessment criteria (e.g. different CARs and attestation letters will be produced to confirm compliance with any standard(s) in addition to the CAR and attestation letter confirming eIDAS compliance);
- The assessment methodology including
    - The sampling methodology;
    - The sites and locations used by the QTSP to provide its QTS (either operated by the QTSP itself or used by third party to which the QTSP outsources the operation of QTS component(s) within the scope of the QTS provisioning) where the different assessment stages will be performed;
    - The list of up-to-date documents, which are required to perform the conformity assessment;

      Note: This includes prior external assessment and/or internal audit reports. Refer to Table 1 for typical list of documents.
    - The effort and time used to conduct the assessment;
    - The effective dates of the assessment stages.
- All necessary arrangements in order to enable the selected CAB to conduct the assessment, including provision for examining documentation and the access to all areas, including those of sub-contractors, records (including internal audit reports and reports of independent reviews of information security) and personnel for the purposes of the assessment, re-assessment audit and resolution of complaints. These necessary arrangements include appropriate access arrangements to confidential or sensitive information and site areas.
- The CAB's team of assessors. Identification of the CAB's allocated assessors may be key to identify potential conflicts of interest, organise access to sites and sensitive areas and/or data, to assess the seniority of assessors involved, etc.
- The need for any involvement of the NAB accrediting the CAB, and/or of the competent SB.

All the above arrangements are recommended to be validated by the competent SB prior to the start of the assessment.

5. CONDUCTION OF THE ASSESSMENT

5.1 STAGE 1

Following the provision by the assessed QTSP of the required documentation, the objective of stage 1 of the assessment is not limited to the review of the documentation as this stage mainly aims to provide a detailed assessment plan for stage 2 by gaining an understanding of the structure and scope of the assessed QTSP/QTS.

In line with the provided documentation and external verifications, stage 1 should include verification of records regarding legal entity, arrangements to cover liability, contractual relationships between the QTSP and its contractors operating or providing QTS component(s), internal/external audits or certifications, security management review, and further investigations with regards to the preliminary review of partial compliances or non-compliances identified in the QTSP self-assessment.[26]

The QTSP shall make sure that the results of audit stage 1 shall be documented by the CAB in a written report including at least, in line with ETSI EN 319 403-1, the following information:

- □ A description of the methodology used to conduct stage 1 (documentation review);
- □ An exhaustive list of the documents and information reviewed during stage 1;
- □ An indication of the audit time (elapsed time) and efforts (man-days) spent on stage 1;
- □ A diagram and a description of the organisational structure of the QTSP/QTS and of the service provisioning architecture of the QTS, including the use made and organisational structure of any external party (e.g. sub-contractor) that provide service component(s) of the assessed QTS;

  Note: This should be a confirmation of the information provided as part of the QTSP documentation on the QTS it provides (see section 4.2 of the present document).
- □ An identification and description of those QTS components that have been evaluated, assessed or certified and their certificates or audit/assessment reports;
- □ An account of the preliminary assessment of the QTSP/QTS against the target assessment criteria, i.e. against the applicable eIDAS requirements, with a focus on:
  - □ an account of the assessment of the information security risk analysis of the assessed QTSP/QTS in line with Art.19.1 of the eIDAS Regulation;
  - □ the identification and description of any areas of concern on whether the assessed QTSP/QTS meet the applicable requirements of the eIDAS Regulation, with an indication whether they are classified as non-conformity or could be classified as non-conformity during stage 2 of the assessment (see also section 5.4 of the present document);
  - □ a brief assessment of the assessor(s) whether stage 2 is likely to succeed; and
  - □ any recommendations regarding the plan for conducting stage 2, including whether additional resources (e.g. technical experts, more auditors) are required for stage 2.

[26] Refer to Table 1 and section 4.2 of the present document for details about the typical list of documents to be provided to and reviewed by the CAB as from stage 1.

The QTSP will receive from the CAB, review and agree:

- □ when necessary, a list of concerns that need to be resolved before execution of stage 2;
- □ the assessment plan for stage 2; and
- □ the type of information and records that are required for detailed verification during audit stage 2.

Any significant change in the assessment plan for stage 2, compared to the assessment plan and methodology previously presented to the SB, should be communicated to the SB.

5.2 STAGE 2

On the basis of stage 1 results and in accordance with the assessment plan for stage 2, the CAB will conduct the second stage of the assessment with the aims:

- to confirm that the QTSP/QTS abide by QTSP's own documentation, and
- to confirm that the implemented QTS conform to the requirements of the applicable assessment criteria, i.e. the applicable eIDAS requirements.

To this extent, the assessors will collect evidences and evaluate the demonstration by the QTSP that the processes, procedures and work instructions are effectively operated and implemented in accordance to the plans, policies and documentation, and that the QTS supported by them, and the QTSP, meet the applicable eIDAS requirements.

5.3 ASSESSMENT REPORT

As a result of the conduction of stage 2, the assessment report shall at least include the following information:

- □ A description of the methodology used to conduct the assessment, including
  - □ the methodology used to conduct stage 1 (documentation review);
  - □ the methodology used to conduct stage 2 (on-site assessment) including:
    - ○ audit enquiries which have been followed, rationale for their selection;
    - ○ sampling methodology; and
    - ○ test procedures.
- □ An exhaustive list of
  - □ the documents and information reviewed during stage 2;
  - □ the visited and assessed sites / locations.
- □ The total audit time (elapsed time) and efforts (man-days) used as well as detailed specification of time and efforts spent on:
  - □ Documentation review with separate indication for stage 1 and for stage 2 when applicable;
  - □ Assessment of risk analysis;
  - □ On-site audit; and
  - □ Assessment reporting.
- □ A (stage 1 updated or confirmed) diagram and description of the organisational structure of the QTSP/QTS and of the service provisioning architecture of the QTS, including the use made and organisational structure of any external party (e.g. sub-contractor) that provide service component(s) of the assessed QTS.
- □ A (stage 1 updated or confirmed) identification and description of those QTS components that have been evaluated, assessed or certified and their certificates or audit/assessment reports.
- □ An account of the results and findings of the evaluation of the conformity of the QTSP/QTS with the target assessment criteria, i.e. against the applicable eIDAS requirements, with a focus on:

- □ The identification of the sites that were audited, the significant audit trails and the audit methodologies used;
- □ Organised as per applicable requirement of the eIDAS Regulation (see CAR-4.2-16 of ETSI TS 119 403-3), an account of the findings, observations made (positive and negative) as well as recommendations for improvement, as applicable;
  - ○ Including an account of the assessment of the information security risk analysis of the assessed QTSP/QTS in line with Art.19.1 of the eIDAS Regulation;
- □ the identification and description of any non-conformities identified, supported by objective evidence (if applicable) and a unique reference to the applicable requirements of the eIDAS Regulation that is not fulfilled; and
- □ comments on the conformity of the QTSP/QTS with the target eIDAS requirements, together with a clear statement of conformity, or non-conformity if this is the case, and, where applicable, any useful comparison with the results of previous audits of the QTSP/QTS.

- □ Information about the samples evaluated during the assessment.
- □ Information about the scope, the description and the results of a significant set of test or production samples and their assessment for all relevant and applicable types of outputs from the assessed QTS.
- □ If these methods are used, completed questionnaires, checklists, observations, logs or auditor notes.
- □ Any additional information required by the SB competent for the supervision of the assessed QTSP/QTS.

In order to provide a basis for the decision to confirm that the assessed QTSP/QTS meet the applicable eIDAS requirements (as targeted assessment criteria), CAB shall produce clear reports that provide sufficient information to support:

- the CAB to make a certification decision, and
- the competent SB to perform a verification that the assessed QTSP/QTS fulfil the requirements laid down in the eIDAS Regulation.

As long as there is any non-conformity to be resolved with regards to the applicable eIDAS requirements as target assessment criteria, there may not be a positive certification decision. It is only in the absence of any non-conformity, that the assessed QTSP/QTS may be certified as conformant to the assessment criteria, in this case to the applicable eIDAS requirements[27].

5.4 NON-CONFORMITIES AND RECOMMENDATIONS FOR IMPROVEMENT

With regards to the findings reported by the CAB (or CAB's assessors), either following stage 1 or stage 2, the assessed QTSP should require the CAB to clearly separate them into non-conformities to the assessment criteria and recommendations for improvement, i.e. between issues that have a direct impact on the certification decision by preventing it (non-conformities) and issues that do not prevent a certification decision but should be resolved or improved be it for security reasons or other reasons (recommendations for improvements).

The CAB may use severity-based notations associated to assessment findings but what matters in the end is whether or not such findings are considered as non-conformities, in which case for a single one of them the certification decision will not be positive.

Would the QTSP decide to continue the evaluation process and solve the reported issues, in particular the non-conformities preventing a certification decision, the QTSP needs to provide the CAB with a so-called "plan of corrective actions". This plan must address each non-

[27] See also note of section 2.5.

conformity and request for improvement reported and for each of them provide a description of the action(s) that will be undertaken to solve the issue and the time to implement the described resolution.

On reception of the plan for corrective actions, the CAB will evaluate the actions described and the time needed to resolve the issues. Consequently, the CAB will inform the QTSP of the additional assessment tasks needed to verify that the non-conformities have been corrected as this will directly impact the certification decision. The planning of the CAB tasks for verifying the implementation of the recommended improvements may differ from the one used to assess the resolution of non-conformities. This might be aligned with assessment actions foreseen in the context of the surveillance program.

Depending on the complexity of the corrective actions for the reported non-conformities, EN 319 403-1 foresees respectively a 3 months deadline for addressing “simple” actions and a 6 months deadline for addressing “complex” actions. In any case, all non-conformities, irrespectively of their severity, must be solved before a positive certification decision may be taken by the CAB.

In case of QTSP being already granted a qualified status for the provision of a QTS, the non-conformities reported in the CAR submitted to the SB, and the resulting absence of certification or absence of confirmation that the assessed QTSP/QTS meet the requirements of the eIDAS Regulation need be accompanied with a plan for corrective actions. Art.20.1 of the eIDAS Regulation requires QTSPs to “*submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it*”. When the SB would confirm any reported non-conformities to be failures to meet the requirements of the eIDAS Regulation, the SB may require the QTSP to remedy such failures within a time limit set by the SB (which may be different than the one required by the CAB). In line with Art.20.2 of the eIDAS Regulation, when the QTSP does not act accordingly or fails to fulfil the eIDAS requirements within the time limit imposed by the SB, the SB taking into account, in particular, the extent, duration and consequences of that failure, may reconsider the imposed time limit when appropriate, or may withdraw the qualified status of the QTSP or of the QTS it provides.

6. CERTIFICATION

6.1 CERTIFICATE / ATTESTATION LETTER

The issuance of a certificate (or attestation letter) conforming (certifying) the conformity of the assessed QTSP/QTS to the applicable requirements of the eIDAS Regulation is subject to:

- The signature of a certification agreement being signed between the CAB and the assessed QTSP, legally engaging the CAB for the provision of the assessment and certification activities and placing obligations on the assessed entity (see ISO/IEC 17065 clause 4.1.2);
- The fulfilment of the certification requirements which include:
  - ○ the target assessment criteria (i.e. the applicable requirements of eIDAS when assessing QTSP/QTS against eIDAS), hence requiring the assessment results having identified not a single non-conformity to these criteria; and
  - ○ other requirements that are additional conditions of establishing or maintaining certification (e.g. completing the certification agreement, paying assessment/certification fees, providing information about changes to the certified QTS, providing access to certified QTS for surveillance activities);
- The decision to grant or extend the scope of certification has been made by the CAB.

The assessed QTSP should verify that the certificate/attestation letter (as well as the accompanying CAR) clearly conveys or permits the identification of:

- □ the name and address of the CAB;
- □ the date certification is granted (the date shall not precede the date on which the certification decision was completed);
- □ the name and address of the QTSP;
- □ the exact scope of the eIDAS certification, i.e.
  - □ a clear identification of
    - □ the type(s) of QTS having been assessed and being certified, referring to nine types of QTS specified by the eIDAS Regulation;
    - □ ideally identifying, in accordance with requirement CAR-4.2-09 of ETS TS 119 403-3 , the service digital identity(ies) per type of QTS for which the certificate and the associated CAR confirm the conformity with the requirements of the eIDAS Regulation;
    - □ ideally identifying the relevant trust service policy(ies), where applicable; and
    - □ when not clearly appearing in the associated CAR, the corresponding content of the applicable national trusted list, which reflects the result of the assessment.[28]
  - □ a clear statement confirming that the identified assessed QTSP/QTS meet all the applicable requirements of the eIDAS Regulation;
- □ the term or expiry date of certification, if certification expires after an established period;
- □ any other information required by the certification scheme;
- □ the identification or reference of the CAS used by the CAB to conduct the assessment;
- □ the identification or reference of the CAR to which the certificate/attestation letter is associated;

[28] Refer to CID (EU) 2015/1505 and ETSI TS 119 612 v2.1.1 for detailed specifications.

- □ the identification or reference of the accreditation of the CAB and the identification of the NAB having issued this accreditation;
- □ the signature or other defined authorization of the person(s) of the certification body assigned such responsibility.

This certification should be issued, at least, in the CAB official national language and in English, be published on the CAB website and kept up to date.[29]

In case of a multi-purpose assessment, there should be as many certificates/attestation letters (and associated CARs) as there are distinct target assessment criteria. For example, when the assessment aimed to confirm the compliance with one or more specific standards in addition to the conformity to the eIDAS requirements, separate CARs and attestation letters will be produced.

6.2 CERTIFICATION / CONFORMITY ASSESSMENT REPORT

The assessed (Q)TSP should verify that the CAR (or certification report):

- □ provides sufficient information to support the competent SB to perform a verification that the assessed QTSP/QTS fulfil the requirements laid down in the eIDAS Regulation;
- □ Meets the recommendations of section 5.3 of the present document, the requirements of ETSI TS 119 403-3 and any additional rightful[30] requirement imposed by the competent SB to which it will be submitted.

As indicated earlier in the present document, in the context of the eIDAS Regulation, a certification of conformity, issued by a CAB duly accredited in accordance with the eIDAS Regulation (see Art.3(18)), of the assessed QTSP/QTS against the eIDAS requirements does not automatically mean that the QTSP/QTS will be granted a qualified status. The final decision on the grant of such a qualified status comes to the competent SB after it has verified that the QTSP/QTS comply with the requirements laid down in this Regulation. The notification to the SB of a CAR confirming that the assessed QTSP/QTS meets the eIDAS requirements is a necessary condition but it might not be a sufficient one. The grant decision by the SB will be based on the CAR and on any additional information/evidence required from the QTSP necessary to verify that the eIDAS requirements are met.

In terms of deadlines associated to the notification of the CAR to the competent SB, this latter has three months, from the initial notification of the CAR and the TSP intention to provide a QTS, to verify that the TSP and the QTS fulfil the eIDAS requirements. However, as per Art.21.2 of this Regulation, "*if the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded*".

With regards to 2-yearly assessments foreseen by Art.20.1 of the eIDAS Regulation, the QTSP must "*submit the resulting CAR to the supervisory body within the period of three working days after receiving it*". The eIDAS Regulation does not place any requirement on any deadline for SB feedback or for any feedback at all. Principles for good administration and relevant national laws may however apply.

[29] Clause 7.7 of ETSI EN 319 403(-1). It is worth noting that a CAB certification of the conformity of the assessed QTSP/QTS with the eIDAS requirements is in no way a confirmation that the assessed QTSP/QTS has been granted a qualified status. Only the corresponding national trusted list brings such a confirmation of the qualified status of a QTSP/QTS.

[30] In respect with good principles of administration and relevant national laws or regulations.

7. SURVEILLANCE AND RENEWAL

7.1 SURVEILLANCE

There is no requirement in the eIDAS Regulation on QTSPs to undertake other regular assessments than the 2-yearly (full) assessments foreseen in its Art. 20.1.

However, pursuant to Art.20.2 of the eIDAS Regulation, the SB in charge of the supervision of a QTSP may at any time (subject to the principles of good administration) audit or request a CAB to perform a conformity assessment of the QTSP, at the expense of the QTSP, to confirm that the QTSP and the QTS(s) it provides fulfil the requirements laid down in this Regulation.

Furthermore, clause 7.9 of ETSI EN 319 403 (and its successor ETSI EN 319 403-1) requires CABs accredited under this standard to define a programme of periodic surveillance and re-assessment. It places requirements on such surveillance audits (e.g. to include on-site audits, to review any changes in documentation and (Q)TSP/QTS operation, to review treatment of complaints, internal audits and ISMS in place) in order to verify that the previously assessed and certified QTSP/QTS continue to comply with the (certification) requirements. The standard recommends that at least one surveillance audit per year is performed in between full assessment audits.

A surveillance audit can also be required by national laws applicable to the QTSP and/or by the SB competent for the supervision of the QTSP.

The certification agreement signed between the QTSP and the CAB also foresees, in addition to the elaboration of a surveillance program, the obligation to notify the CAB with any change that may affect the certification. In case of such change being notified, the CAB will determine and communicate to the QTSP the appropriate conformity assessment activities needed to assess that ongoing conformity is given. Notification and decision must be performed before implementation of the measures. This latter requirement from EN 319 403(-1) needs to be correctly reflected in the QTSP documentation related to the provision of its QTS(s) including details about timing, threshold for notifying, etc.

Depending on the nature and importance of the change (e.g. major changes to the documentation or operation of the assessed QTS), a full re-assessment of the previously assessed QTSP/QTS may be required (see clause 7.9 of ETSI [EN 319 403-1][).

Changes to the operations of a QTS for which a QTSP has been granted a qualified status must also be notified to the competent SB (as well as intention to terminate such QTS) in line with point (a) of Art.24.2 of the eIDAS Regulation. Following the notification and verification of the significance of such changes, the SB may decide to audit or request a CAB to perform a conformity assessment of the QTSP to confirm that the QTSP and the QTS(s) it provides fulfil the requirements laid down in this Regulation.

7.2 RENEWAL

The (full) re-assessment of the previously assessed QTSP/QTS shall be conducted the same way as for an initial assessment while taking into account the results of the previous assessment(s).

8. CONCLUSIONS

Assessments of QTSPs and the QTS(s) they provide to confirm they fulfil the applicable requirements of the eIDAS Regulation are required throughout the life cycle of the provision of such QTS(s), from their genesis until their termination. These assessments may be lengthy and costly due to the level of preparation and maturity that is required to address them. The more guidance (prospective) QTSPs may receive on these aspects, the better.

This document aims to provide this guidance by presenting an overview of the conformity assessment framework for (prospective) QTSPs in the context of the eIDAS Regulation, and discussing the typical process flow and the methodology used to perform conformity assessments. For each phase of the assessment, guidance is provided to (prospective) QTSPs for the purpose of preparing and undertaking the conformity assessment, as required by the eIDAS Regulation, in the best possible conditions.

9. REFERENCES

9.1 STANDARDS

ID	Description
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 EN 319 403-1	ETSI EN 319 403-1 V2.3.1 (2020-04): "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 319 421	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".
ETSI EN 319 422	ETSI EN 319 422 V1.1.1 (2016-03): "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
ISO 9001	ISO 9001:2015: “Quality management systems — Requirements”.
ISO/IEC 17065	ISO/IEC 17065:2012: "Conformity assessment — Requirements for bodies certifying products, processes and services".
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”.
RFC 3647	IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

9.2 ENISA PUBLICATIONS

ID	Description
ENISA - QTSP standards	Recommendations for QTSPs based on standards. Technical guidelines on trust services. https://www.enisa.europa.eu/publications/reccomendations-for-qtsps-based-on-standards/
ENISA - Art.19	Article 19 Incident reporting - Incident reporting framework for eIDAS Article 19. https://www.enisa.europa.eu/publications/article19-incident-reporting-framework
ENISA - TSP security	Security framework for trust service providers. https://www.enisa.europa.eu/publications/security-framework-for-trust-providers/
ENISA - QTSP security	Security framework for qualified trust service providers. https://www.enisa.europa.eu/publications/security-framework-for-qualified-trust-providers

ENISA - QTS initiation	Guidelines on Initiation of Qualified Trust Services - Technical guidelines on trust services. https://www.enisa.europa.eu/publications/tsp-initiation
ENISA - QTS supervision	Guidelines on Supervision of Qualified Trust Services - Technical guidelines on trust services. https://www.enisa.europa.eu/publications/tsp-supervision
ENISA - QTS termination	Guidelines on Termination of Qualified Trust Services - Technical guidelines on trust services. https://www.enisa.europa.eu/publications/tsp-termination
ENISA - CAS	Towards a harmonised conformity assessment scheme for QTSP/QTS. https://www.enisa.europa.eu/publications/towards-a-harmonised-conformity-assessment-scheme-for-qtsp-qts

9.3 APPLICABLE LEGISLATION

ID	Description
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
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
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

ANNEX A. FAQ

A.1 WHICH CAB TO SELECT IN THE CONTEXT OF EIDAS ASSESSEMENTS?

The CAB must be accredited in line with the requirements of Art.3(8) of the eIDAS Regulation.

The European Commission compiles a list of CABs accredited against the requirements of the eIDAS Regulation, which is available on Futurium.[31]

Before contracting a CAB, QTSP should refer to the guidance provided in section 4.3 of the present document.

A.2 WHAT SHOULD BE THE SCOPE OF AN EIDAS ASSESSMENT?

The assessment, the resulting certificate/attestation letter and CAR shall be respectively conducted and issued to confirm - if such is the case - that the assessed QTSP/QTS meet all the applicable requirements of the eIDAS Regulation. This means that the normative document is the eIDAS Regulation itself and the target assessment criteria are the eIDAS requirements applicable to the QTSP and the (type of) QTS it provides or intends to provide.

Compliance against standards does not automatically imply conformance to eIDAS requirements. Although these standards may be seen as best practices, there is no automatic presumption of compliance to eIDAS when meeting the said standards. Hence the scope of an eIDAS conformity assessment shall never be any standard per se but shall be the applicable QTSP/QTS requirements from the eIDAS Regulation itself.

A.3 WHAT SHOULD AN EIDAS CONFORMITY ATTESTATION LETTER LOOK LIKE ?

The main requirement for an eIDAS conformity attestation letter is to include a clear statement confirming that the assessed QTSP/QTS identified by the letter meet all the applicable requirements of the eIDAS Regulation.

The attestation letter needs to include additional information, including those aiming to identify the CAB, its valid accreditation by a NAB in accordance with the eIDAS Regulation, the concerned NAB, the CAS used to conduct the assessment, the validity period of the attestation.

Refer to the guidance provided in section 6.1 of the present document.

A.4 WHAT SHOULD AN EIDAS CONFORMITY ASSESSMENT REPORT LOOK LIKE ?

In a nutshell, an eIDAS conformity assessment report should be compliant with ETSI TS 119 403-3.

Refer to the guidance provided in section 6.2 of the present document.

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

A.5 WHICH ENTITY IS THE SB COMPETENT FOR THE SUPERVISION OF A QTSP/QTS?

The entity that is competent for the supervision of a QTSP/QTS is the body designated as “supervisory body” by the EU Member State in which the QTSP is established.

The identification data (incl. the name, physical and electronic addresses) of the EU MS supervisory bodies can be found in the EU MS trusted lists. The EC provides “Trusted List Browser” as a tool to browse these national eIDAS trusted lists and the EU List of Trusted Lists (LOTL).[32]

A.6 WHEN SHOULD THE SB BE INVOLVED IN THE CONTEXT OF EIDAS ASSESSEMENTS?

QTSPs are recommended to involve the competent SB as soon as possible in the process of an eIDAS assessment, and throughout its various phases. Refer to the guidance provided in section 3 of the present document.

A.7 WHAT DOCUMENTATION SHOULD BE READY BEFORE AN EIDAS ASSESSEMENT?

Depending on the type of QTS provided and on the scope and size of such a provision, the documentation can be significant both in terms of quantity and complexity. The documentation should provide sufficient information to demonstrate that the QTSP/QTS meet the high-level security and provisions of the eIDAS Regulation. It should cover all aspects of the provision of the QTS(s) provided by the QTSP and the relevant data on the QTSP itself. A self-assessment on the demonstration that the QTSP/QTS fulfil the eIDAS requirements should be part of the documentation. Refer to the guidance provided in section 4.2 and Table 1 of the present document for a typical list of documents to be provided as from stage 1 of the assessment.

With regards to confidential or sensitive information, the key principle is that, if the CAB concludes that access to an information is required to demonstrate and warrant an effective audit, then the QTSP needs to accept and arrange appropriate access to this confidential or sensitive information. If not, the conformity assessment may not take place.

A.8 HOW LONG / INTENSE SHOULD AN EIDAS ASSESSEMENT BE?

There is no requirement in the eIDAS Regulation on the duration or on the effort a CAB must spend in the conduction of an assessment of the conformity of a QTSP and the QTS it provides with the requirements of this Regulation.

These duration and effort should however be sufficient to bring confidence to the SB and sufficient credibility that the results of such an assessment demonstrate actual conformity to eIDAS. Some EU MS SBs or NABs may define specific requirements on the minimum duration and efforts for the conduction of QTSP/QTS eIDAS conformity assessments, such as in Italy[33] (leveraging on the audit time calculation table of ISO/IEC 27001) or Luxembourg[34]. ETSI EN 319 403-1 lacks specifications or guidance on minimal figures for such duration and efforts in its informative Annex B on a Procedure to determine audit time. No harmonised guidance is provided at EU level (e.g. by EA, by ESOs).

Refer to section 4.4 for discussion on additional organisational aspects of conformity assessments.

[32] https://webgate.ec.europa.eu/tl-browser/
[33] ACCREDIA – Circolare Tecnica N. 5/2020 Rev.02 - Circolare per l’Accreditamento a fronte del Regolamento Europeo 910/2014 (eIDAS) – 16.03.2020.
[34] ILNAS/PSCQ/Pr001 - Version 5.0 – 22.09.2017 – Clause 8.

A.9 IS IT POSSIBLE TO COMBINE A QTSP/QTS AUDIT AGAINST EIDAS WITH OTHER AUDITS AGAINST OTHER TARGET CRITERIA?

QTSPs may need to deal with assessments against several target criteria in addition to the applicable requirements of the eIDAS Regulation. For example, they may need to have the provision of qualified certificates for website authentication be assessed for their conformance with CA/B Forum requirements and browser vendor's specifications. QTSPs may also need to have the compliance of their provision of QTSs been certified against standards.

As a general principle, QTSPs should make sure that an assessment is conducted, and the resulting certification is issued, with regards to the appropriate specific target criteria, by a CAB that is appropriately accredited for that scope.

QTSPs should be cautious when willing an assessment to be conducted with multiple purposes; contracting an auditor to assess, during the same audit period, the conformity of a QTSP/QTS with different sets of requirements is possible but this may require as many separate certification attestations (certificates) and certification reports as there are different assessment targets. It is however possible to mutualise audit time and tasks when requirements are common to different targeted sets and align resulting CARs but these latter must be consistent to the assessment purposes and may each be required specific content and structure.

ANNEX B. DOCUMENTATION OVERVIEW

B.1 INTRODUCTION

Section 4.2 of this document presents, under the form of a (check-)list (cf. Table 1), the typical documentation that the QTSP should establish and maintain in the context of the provision of its QTS(s), and that should be provided or made accessible to the CAB as from stage 1 and reviewed by the CAB during the assessment.

The aim of Annex B is to further give a short overview and description of that typical documentation, which includes:

Clause B.2 Documentation describing the company and the way it organised the governance of the provision of QTS and contracting partners, customers, relying parties,

Clause B.3 Documentation describing how the QTSP/QTS comply with the eIDAS Regulation, when applicable with other regulations,

Clause B.4 Description on how the QTSP/QTS comply with standards,

Clause B.5 Documents stating the policies and practices used for the provision of QTS, and

Clause B.6 Documentation related to the technical implementation and management of such QTS provision, including relevant plans, policies, processes, procedures, work instructions as well as records and/or logs evidencing their implementation.

An index structuring the access to the documentation is recommended to be maintained and provided to the CAB together with the documentation.

In order to support the establishment and management of the recommended documentation and more generally to support the provision of QTS in line with eIDAS, QTSP can refer to ENISA report on "*Recommendations for QTSPs based on standards*" [ENISA - QTSP standards], which provides recommendations to help QTSPs and auditors understanding the expected mapping between the eIDAS requirements/obligations applicable to QTSP/QTS and reference numbers of standards, as well as practical recommendations for their usage.

B.2 QTSP COMPANY DOCUMENTATION

Legal statutes / Memorandum and Articles of Association and other **extracts of official registers** will aim to confirm the existence, the official name (as well as official abbreviation(s) and/or short name(s)) and, when applicable, the registration number of the legal person acting as QTSP.

Company blue prints aim to provide a description of the external and internal organisation of the QTSP as a company. The external organigram includes the description of the company shareholders and the entities the company is having shares of. A mapping between such an external organigram and the external entities that are involved in the operations or provision of QTS service components could also be provided. The internal company organisation should include a clear description of the internal organisation and organigram of the company, down to identifying the name and functional roles of the company subdivisions, and of the personnel, in particular the (trusted) personnel involved in the operations and implementation of the QTS the company provides (or intends to provide) as a QTSP.

Information on the QTSP's economic resources aims to demonstrate the financial capability of the QTSP to sustain the provision of its QTS(s), with regard to the risk of liability for damages (e.g. resulting from faults, incidents, failures). This information typically includes audited financial statement (e.g. for the last 3 years) and evidence of liability insurance and/or of capital adequacy for the provision of QTS. The enclosed information must be able to show sufficient economic resources to be able to run a business in accordance with the requirements laid down in eIDAS Regulation and national laws for QTSP/QTS (cf. point (c) of Art.24.2 of eIDAS).

An organization exists as a system of coordinated activities accomplishing its defined goals and objective according to the defined strategy. For this purpose, clear roles and responsibilities must be defined and assigned to personnel, based on their place in the hierarchy, in order to perform their tasks efficiently. The documentation regarding the **organisation of the QTS management by the QTSP** mainly focuses on:

- The identification and description of the instrument (e.g. virtual or structural group of empowered resources) that is empowered by the QTSP to manage and have managerial decisions on the provision of its QTS(s). The PKI literature usually refers to that instrument as the “TSP’s management”, the “TSP managerial body” or the “PMA” (Policy/PKI Management Authority). The related documentation should include the PMA composition, its internal rules of procedures, as well as meeting and decision records.
- The overview and functional description of the organisational structure of the provision of the QTS(s) by the QTSP, including information on the roles and responsibilities allocated to identified personnel/staff either internal or external to the QTSP) including the identification of the external contractors/partners involved in the provision of QTS components, their roles and responsibilities. It should also include or reference recommendations enforcing security measures as well as methods to maintain the personnel discipline.

The QTSP should further document all the relevant **(contractual) agreements** it has set up and signed to support the provision of its QTS(s). This includes:

- Agreements with (sub-)contractors and/or partners for the provision of QTS, incl. service components;
- General terms and conditions, towards customers and relying parties;
- The general template(s) and signed/approved version of the customer agreements (e.g. contracts).

B.3 CONFORMITY TO EIDAS (AND WHEN APPLICABLE, WITH OTHER REGULATIONS)

This documentation category mainly addresses the eIDAS conformity self-assessment prepared and maintained by the QTSP to facilitate the demonstration that the QTSP/QTS fulfil the applicable requirements of the eIDAS Regulation. eIDAS self-assessments may be supported by a self-assessment check-list structured around the applicable requirements following the numbering of the relevant articles of eIDAS. This check-list should be aligned with the list of checks used by the CAB to evaluate the assessed QTSP/QTS for its conformity with eIDAS and the CAR structure as required in ETSI EN 319 403. ENISA report on “*Recommendations for QTSPs based on standards*” [ENISA – QTSP standards] provides further guidance on the standards and standardised check-lists that can be used for that purpose.

The documentation may also include, when applicable and appropriate, attestations of conformity with other relevant national, regional, or international regulations, whether public (e.g. legislation based) or private (e.g. Industry based).

B.4 COMPLIANCE WITH STANDARDS

This documentation refers to the list of standards to which operations have been positively audited, evaluated, certified or assessed to be compliant. It should also provide, for each such standard conformity assessment, the associated certificates of conformity, and details about the underlying audit, evaluation, certification or assessment scheme. This may point to certification against ISO/IEC 27001 and/or ISO/IEC 27701, or certification against relevant ETSI or CEN standards. ENISA report on "*Recommendations for QTSPs based on standards*" [ENISA - QTSP standards] provides further guidance on the ETSI/CEN standards that can be useful to build the provision of QTS and whose compliance may facilitate the demonstration of conformity to the eIDAS requirements.

A list could also be provided of additional standards with which operations are claimed to be compliant but for which no external attestation of conformity is available. When internal assessment or external (non-conclusive) evaluation have been performed, the associated reports should be part of this documentation set.

B.5 POLICIES AND PRACTICES USED FOR THE PROVISION OF QTS

The primary "entry point" documentation used by relying parties and more specifically CABs to evaluate the trustworthiness and/or the compliance of a QTSP/QTS with a said set of requirements are:

- The **trust service practice statement** declaring the practices that a QTSP employs in providing a QTS, and
- The associated **trust service policy(ies)**, meaning the set(s) of rules that indicates the applicability of a trust service to a particular community (e.g. a nation or geographical region, specific market or industry sector of activities) and/or class of application with common security requirements (e.g. organised under various levels of security, assurance or reliability).[35]

The most commonly known instantiation of a trust service practice statement and trust service policy are respectively the certification practice statement (CPS) and the certificate policy (CP) in the context of the provision of digital certificates. The concept, may, however be extended, as defined and specified in the relevant ETSI standards, to all types of trust services building upon and extending the RFC 3647 specifications for the content of CP and CPS.

In general, the purpose of a trust service policy is to state "what is to be adhered to" when providing the trust service while a trust service practice statement states "how it is adhered to", i.e. the processes and practices used by the QTSP when providing the QTS. A trust service policy can be a "higher level" document than a trust service practice statement in the sense that it can apply to a community to which several QTSPs abide by the common set of rules specified in that trust service policy. A trust service practice statement defines how one specific QTSP meets the technical, organizational and procedural requirements identified in a referenced trust service policy. The latter is usually defined independently of the specific details of the specific operating environment of a QTSP, whereas the practice statement is tailored to the organisational and operational environment of a provider. A QTS policy can be defined by a third party, external to the TSP, whereas the QTS practice statement is always defined and owned by the provider.

[35] As defined in ETSI EN 319 401.

These trust service policy and practice statement are common entry points for most conformity assessments of a QTSP/QTS, because they aim to include, directly or by reference when sensitive data is concerned, lower-level documentation detailing the specific details, including specific plans, policies, processes, procedures and work instructions necessary to complete the declaration of practices identified in the practice statement to provide the QTS in accordance with the identified trust service policies.

Trust service policy and practice statement documents must provide enough detail to allow third parties to assess how QTSPs enforce imposed or targeted requirements (e.g. eIDAS, CA/B Forum Baseline Requirements). A section of those documents that simply notes its compliance with the applicable requirements is insufficient.

B.6 QTSP/QTS TECHNICAL DOCUMENTATION

B.6.1 General documentation

The general documentation on the technical aspects should start with a general overview of the scope of the QTS provided, of the technical and organisational blueprints, of the used locations/sites, of the QTS size, of the service components and of the associated (sub-)contractors. This general overview should be supported by visuals or diagrams, which should also, when relevant, be included in the trust service practice statement.

Documents presenting the QTS detailed architecture should be provided as well including overview of the high-level and low-level designs of the infrastructure used to provide the QTS with references to further detailed documentation available in the detailed technical documentation.

When PKI-based technology is used to support the provision of the QTS, a detailed visual representation of the PKI hierarchy used should be provided along with the identification of the root, intermediate and signing authorities and/or units involved in the QTS provision.

The general technical documentation should be completed by the detailed and complete description of the technical, physical and logical infrastructure used by the QTSP to provide its QTS(s). This may include, when applicable, security qualification (like Common Criteria or FIPS 140-3 security certificates) of cryptographic key management technical components used by QTSP for QTS provision.

B.6.2 Plans, policies, processes, procedures, work instructions and evidences for the provision of QTS

Plans are high-level statements that aim at providing a clear understanding of the long-term objectives defined by the QTSP throughout the organization and are periodically reviewed and updated by the management.

Policies are principles, rules or guidelines established and adopted by Trust Service Providers to influence or determine the way of proceeding in specific cases or areas, in line with the established plans.

In order to concretely implement the provision of QTS in line with the plans and policies, QTSPs need to define processes, procedures and work instructions supporting such implementation, where (cf. ISO 9001):

- An overall **process** (hierarchy) description shows the chain of activities that use resources to transform inputs into outputs (cf. ISO 9001). In case of QTS provision, it means the chain of activities aimed to achieve the goals of the plan in line with the associated policy(ies).

- Existing **procedures** describe the specified way to carry out the activities of the process, and
- Existing “**work instructions**” describe in detail how an activity within a process (or procedure) is performed.

Plans, policies, processes, procedures, work instructions and evidences established and maintained for the provision of QTS, applicable to the provision of the QTS as a whole and/or on the basis of its service components in line with the type of QTS, can be grouped in logical areas, including:

1. QTS Infrastructure Management
2. QTS provision operations
3. Data privacy and GDPR
4. Security
5. Incident
6. Communication
7. Business continuity
8. Contingency
9. Disaster recovery
10. Termination
11. Legal enforcement
12. (Trusted) personnel
13. Testing
14. Internal audit / quality monitoring
15. External audits
16. Recording and archival

B.6.2.1 QTS Infrastructure Management

In order to respond to the continuous evolution of the QTSP strategic and business plans associated to the provision of QTS, as well as the evolution of the planned/deployed infrastructure in terms of technology, best practices, associated risks and threats, etc., QTSP should establish and maintain a plan and associated policy(ies) to manage and monitor the entire infrastructure, whether software or hardware including servers (e.g. CPU, storage, memory), databases (e.g. table spaces, data files, file systems), networking devices, and security controls (e.g. firewalls, intrusion prevention systems).

This should include documentation on the management of changes made to the infrastructure. QTS provisioning systems require frequent changes, e.g. due to software packages added, removed or modified, or because of the introduction of new hardware. Proper management of these changes is required in order to perform maintenance activities in a controlled way and ensure the integrity of the necessary systems as well as the continuation of the QTS to meet its service requirements and expectations. QTSPs should indicate the scope of the affected system(s) (e.g. on test, production) and of the kind of modification (e.g. permanent changes, temporary changes, emergency changes) and the procedure associated to it. All these requirements should be defined accordingly and a responsible person should be designated for every asset. These procedures should serve a defined process workflow including at least:

- identification of the change (e.g. affected services);
- technical evaluation and risks associated to the change;
- approval of the change;
- information of the change (e.g. according to the communication policy);
- execution of the change;
- new testing to validate the change.

For recovery and integrity purposes, a detailed inventory of the hardware and software is necessary.

QTSPs should define the processes, procedures and work instructions, supporting the correct implementation of the QTS infrastructure management (incl. change management) plans and policies. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

B.6.2.2 QTS provision operations

The provision of QTS can be seen as a system of activities coordinated to accomplish defined goals and objectives according to the defined strategy. The operation of the provision of a QTS can be organised and split in terms of service components whose functional roles, responsibilities and operational task collectively aim to properly implement this system of activities.

For this purpose, clear roles, responsibilities and tasks must be defined and assigned to each service component and to the associated personnel, including recommendations enforcing security measures as well as methods to maintain the personnel discipline.

QTSPs should define the processes, procedures and work instructions, supporting the correct implementation of the plans and policies ruling the QTS provision operations. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

B.6.2.3 Data privacy and GDPR

QTSPs should define and maintain plans, policies and associated processes, procedures and work instructions, addressing the management of personal data and demonstrating the fulfilment of the requirements of the General Data Protection Regulation [GDPR] in the context of the provision of QTS. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

[ISO/IEC 27701] is an extension of [ISO/IEC 27001] for Privacy Information, which extends an ISMS (Information Security Management System) into a PIMS (Privacy Information Management System). [ISO/IEC 27701] may be seen as a framework for managing data privacy, and so may be seen as a tool to reach compliance to GDPR, demonstrating that the TSP is “in control” regarding data privacy. It is worth noting that being certified against [ISO/IEC 27701] is by no means a presumption of compliance to GDPR, and similarly that GDPR does not mandate the certification or the compliance to the [ISO/IEC 27701] standard. Furthermore, in order to be useful in the context of demonstrating compliance with Article 5 of eIDAS, the scope of [ISO/IEC 27701] certification (the same applies for [ISO/EC 27001] certification) should explicitly address the provision of the QTS(s) by the QTSP.

B.6.2.4 Security

A security plan, or set of plans, support QTSPs in ensuring the continuous protection of their assets and resources (including but not limited to IT resources) by providing a clear overview of the security requirements and describing the management, operational as well as technical controls in place.

The security plan(s) plan should also address security “sub-areas” including:

- The inventory of assets;
- The management of risks;
- Information security management;
- Physical security management;
- Access control management.

For the creation of their security plan, QTSPs should follow existing standards such as ISO/IEC 27001 (or equivalent) and make sure it is aligned with other plans such as contingency plan, disaster recovery plan, business continuity plan or incident management plan. The use of such standards and in particular any certification of conformity should not be limited to the global security aspects of the QTSP as a company but should scope specifically the provision of QTS. This principle applies to all security plan or sub-plans identified in the above list, as well as to the associated policies (ruling the way of proceeding in those specific security sub-areas in line with the established plans) as well as the associated processes, procedures and work instructions supporting the proper implementation of these security plans and policies. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

The ENISA report on "*Security Framework for QTSPs*" [ENISA - QTSP security] proposes a security framework for QTSPs, on top of the one proposed for TSPs (cf. [ENISA - TSP security]) taking into account the type of QTS provided, regarding policies, procedures, and processes in order to be compliant with the security requirements defined in eIDAS under Article 19.

B.6.2.5 Incident management and notification

QTSPs should define and maintain plans, policies and associated processes, procedures and work instructions, addressing the management and notification of incidents in the context of the provision of QTS (e.g. incidents impacting the QTS infrastructure, affecting the normal QTS operations). QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

Further guidance on incident management and incident notification can be found respectively in ENISA reports "*Security framework for QTSPs*" [ENISA - QTSP security] and on "*Incident reporting framework for eIDAS Article 19*" [ENISA – Art. 19].

B.6.2.6 Communication

QTSPs should define and maintain plans, policies and associated processes, procedures and work instructions, addressing all communications to be undertaken in the context of the provision of QTS. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

Proper management of communication is key in order to ensure an efficient exchange of all required information internally but also outside the QTSP organisation. Communication plan(s) should address the type of information exchanged, define the target audience, and identify the potential impacts on the QTSP/QTS.

Based on the target audience and the type of information to be exchanged, QTSPs may categorize communication as follows:

- Internal communication (e.g. to employees and staff);
- Business communication (e.g. to customers, to relying parties);
- Emergency communication (incl. incident or data breach notification, disaster, business continuity, termination of activities);
- Communication to competent SB (incl. notification of intention to provide QTS, notification of changes in the provision of QTS and/or cessation of activities, dialogue in the context of conformity assessments)
- Media communication;
- Shareholders communication.

B.6.2.7 Business continuity

In order to ensure the preservation of its business (e.g. trust services) during and after major disruption, QTSPs should have a well-defined business continuity plan as part of its response planning. This plan aims at describing all the arrangements foreseen by QTSPs, including processes and procedures, to recover as quickly as possible from any kind of major disruption regarding its network or its systems and continue to provide its services.

The business continuity plan should be maintained, tested and be subject of training. As part of its implementation, this plan will require the creation of two other plans: a disaster recovery plan and a contingency plan.

QTSPs should define and maintain the relevant policies and associated processes, procedures and work instructions, addressing business continuity and supporting the business continuity plan in the context of the provision of QTS. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

B.6.2.8 Contingency

A contingency plan defines all the interim measures, such as the relocation of systems to a back-up site, which are in place to help QTSP recover from a disaster and ensure the continuation of its services. This plan can include several phases including detection, notification, evaluation and resolution, which must be described and checked.

QTSPs should define and maintain such a plan, applicable policies and associated processes, procedures and work instructions, addressing contingency in the context of the provision of QTS. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

B.6.2.9 Disaster recovery

The disaster recovery plan defines the technical and functional requirements to protect the IT infrastructure of a QTSP and restore its operability following a disaster.

Analysis and availability of critical recovery resources is important in order to develop the ongoing recovery cost estimates. There should be specific recovery strategies defined for IT as well as business processes.

Some requirements to consider regarding the IT infrastructure include:

- systems hardware resources;
- systems data storage requirements;
- unique (i.e. non-standard) hardware resources;
- distributed systems (e.g. workstations, extranet, intranet, etc.).

QTSPs should define and maintain such a plan, applicable policies and associated processes, procedures and work instructions, addressing recovery from disaster in the context of the provision of QTS. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

B.6.2.10 Termination

A termination plan is a key document regarding a QTSP/QTS because of its particular importance regarding the sustainability and durability of the QTS(s) provided and to increase users’ confidence in the preservation over time of the legal effect associated to QTS received, despite their cessation including in exceptional/unfortunate cases of QTSP unscheduled termination (e.g. bankruptcy)

Article 17(4) and Article 24.2(j) of the eIDAS Regulation require the termination plan to be maintained up to date and be available for verification by the SB because of its particular importance.

The termination plan should contain at least information on affected entities, reliable party (parties) to which TSP obligations will be transferred, as well as a detailed procedure of notification and transfer including a timing aspect with all affected parties taken into consideration.

The ENISA "*Guidelines on Termination of Qualified Trust Services*" [ENISA - Termination] provides further guidance on the termination obligations and activities, the exploration of a set of possible termination scenarios, and a proposed structure for the content of a termination plan.

QTSPs should define and maintain such a termination plan, the applicable policies and associated processes, procedures and work instructions, addressing the cessation of activities related to the provision of QTS. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

B.6.2.11 Legal enforcement

QTSPs should have a clear plan and associated policy(ies) to address the major legal obligations at national and international level, which can affect the services provided.

Besides the eIDAS Regulation, QTSPs may be subject to other applicable laws and regulations such as:

- National laws related to the provision of trust services;
- Personal data protection laws;
- Contract laws;
- Industry or sectorial regulations.

QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

B.6.2.12 (Trusted) Personnel

QTPSs should have a clear plan and associated policy(ies) to address the management of (trusted) personnel involved in the context of the provision of QTS. Personnel refers to internal resources (e.g. employees) and to external resources (e.g. consultants, contracted parties and staff).

QTSPs may categorize the (trusted) personnel plan into sub-plans and associated policies to address specific topics, including:

- (Trusted) personnel recruitment;
- (Trusted) personnel tasks allocation (in line with documented "job descriptions");
- (Trusted) personnel training.

Given the complexity of the environment of QTSP/QTS, all personnel (internal and external) should be educated and receive appropriate training for the most important aspects of QTS operations, and more specifically on the tasks they have been allocated. For this purpose, the QTSP should define a clear plan describing the type of trainings required and how they can be given according to the target audience. Trainings should be given to the (trusted) personnel in line with their roles and responsibilities in the context of the QTS provision.

QTSPs should define and maintain such plan(s), the applicable policies and associated processes, procedures and work instructions, addressing the management of (trusted) personnel in the context of the provision of QTS. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

B.6.2.13 Testing

QTPSs should have a clear plan and associated policy(ies) to address testing in the context of the provision of QTS. QTSPs may categorize the (trusted) personnel plan into sub-plans and associated policies to address mainly two categories of testing:

- The testing of the outputs of the QTS they provide e.g. for the verification of their conformance to QTSP specifications, to standards, to regulatory requirements including the applicable eIDAS requirements; and
- The testing of the execution of documented plans, and of the efficiency of the associated processes, procedures and work instructions to support such execution in line with the relevant policies.

Tests should be quantitatively and qualitatively sufficient to cover all or the vast majority of potential positive and negative test cases to demonstrate the correctness and pertinence of the expected results of the provision of QTS.

Useful resources for testing interoperability and conformance of QTS with ETSI ESI standards are provided in the ETSI TS 119 xx4 series of documents in particular with regards to digital signature formats, to the provision of electronic delivery services and registered electronic mail services. Furthermore, with regards to QTSP providing qualified validation of qualified electronic signatures/seals, the European Commission has made available test cases for assessing an implementation of electronic signatures and seals validation[36] by means of a web site hosting 100+ test cases[37] that can be used by a TSP or by any conformity assessment body or supervisory body to verify or demonstrate the conformity a validation service with the eIDAS requirements.

The testing of the execution of documented plans, and of the efficiency of the associated processes, procedures and work instructions to support such execution in line with the relevant policies should be organised on a regular basis for the most critical plans, e.g. disaster recovery plan, termination plan, incident notification plan. Some good examples of such testing are vulnerability tests, penetration tests, disaster recovery tests.

QTSPs should define and maintain such plan(s), the applicable policies and associated processes, procedures and work instructions, addressing the management of (trusted) personnel in the context of the provision of QTS. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

B.6.2.14 Internal audit / quality monitoring

QTSPs should define and maintain plans, policies and associated processes, procedures and work instructions, addressing the management of internal audits and quality monitoring in the context of the provision of QTS. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

B.6.2.15 External audits

QTSPs should define and maintain plans and relevant policy(ies) addressing the contracting and the conduction of external assessments of the conformity of the QTSP/QTS with applicable regulations (including eIDAS) and selected standards and/or Industry specifications, when applicable. QTSPs should collect and document the associated evidences, records, and/or logs demonstrating their correct implementation.

[36] Hosted by the European Commission and currently available via https://webgate.ec.europa.eu/esig-validation-tests/testcases

[37] Variations of cases are based on combinations of the certificate content, trusted list content, pre/post-eIDAS time of signing, etc.

B.6.2.16 Recording and archival

QTSPs should define and maintain plans, policies and associated processes, procedures and work instructions, addressing the recording and archival of evidences, records and logs in the context of the provision of QTS. QTSPs should collect and document the collected evidences, records, and/or logs demonstrating their correct implementation.

The recording and archival policy is an internal document maintained by Trust Service Providers to define the rules regarding the recording and archival of critical information, due to either business or legal requirements. It sets the rules regarding the recording and archival processes, specific to the type of data to be recorded and archived. It includes information such as the recording and archiving criteria, mechanism and storage used, retention period as well as the person(s) authorized to perform the recording and/or the archival.

Evidences and logs are collected with the purpose of providing details regarding an event and demonstrating the effectiveness of associated processes, procedures and work instructions. Measurement of this information provides the ability to improve them. For every defined plans, policies and associated set of processes, procedures and work instructions, QTSPs should obtain evidence that the related documents are consistently followed up. For this purpose, tools can support QTSPs in the execution of specific tasks, and provide efficient management of all analogous information.

In order to ensure the effectiveness and proper functioning of the resources, evaluation of all hardware and software in place at the QTSP should be performed on a regular basis, generating evaluation reports as well as evidence that should be recorded and appropriately archived. Evaluation reports can also be generated following other types of activities such as personnel trainings (e.g. tests) or audits (e.g. findings).

Logging events can help QTSPs in tracking issues and finding the root causes in case of incidents such as system failures or security breaches. For this purpose, all the logs generated by a system with regards to specific events should be recorded and stored accordingly.

10.2824/785453

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally 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: 978-92-9204-437-4
DOI: 10.2824/785453