THE EU CYBER SECURITY AGENCY

GUIDELINES ON INITIATION hC v ¦ ! [LCL95 ¢w ¦ {¢ {9w±L/9S

Technical guidelines on trust services

DECEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use trust@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to thank all those who contributed to this study and reviewed it, specifically the experts and the members of national supervisory bodies, conformity assessment bodies and various trust service providers.

ISBN: 978-92-9204-189-2
DOI: 10.2824/238163

Table of Contents

Abbreviations

CA	Certification Authority
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CD	Commission Decision
CEN	Centre Européen de Normalisation
CID	Commission Implementing Decision
CIR	Commission Implementing Regulation
EA	European co-operation for Accreditation
EC	European Commission
EEA	European Economic Area
eID	electronic Identification
EN	European Standard
ESO	European Standardisation Organisation
ETSI	European Telecommunications Standards Institute
ETSI TS	ETSI Technical Specifications
EU	European Union
IAS²	IAS² European Commission Study – SMART 2012/0001 (see bibliography)
ISO	International Organization for Standardization
MLA	Multilateral Agreement
MS	Member State
NAB	National Accreditation Body
OID	Object Identifier
OJ	Official Journal (of the European Union)
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
SB	Supervisory Body
Sdi	Service digital identifier
SME	Small and Medium-sized Enterprise
TL	Trusted List
TLSO	Trusted List Scheme Operator
TS	Trust Service
TSA	Time Stamping Authority
TSP	Trust Service Provider
TSP/TS	Trust Service Provider and the Trust Service it provides
TSU	Time Stamping Unit
URI	Uniform Resource Identifier
QWAC	Qualified Website Authentication Certificate

1. General context/the eIDAS Regulation on eID and trust services

1.1 Introduction

Regulation (EU) No 910/2014[1] (hereafter the **eIDAS** Regulation), on electronic identification and trust services for electronic transactions in the internal market, provides a regulatory environment for electronic identification of natural and legal persons and for a set of electronic trust services, namely electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication[2].

The eIDAS Regulation sets the principle of non-discrimination of the legal effects and admissibility of electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and electronic documents as evidence in legal proceedings. Courts (or other bodies in charge of legal proceedings) cannot discard them as evidence only because they are electronic but have to assess these electronic tools in the same way they would do for their paper equivalent.

Whether you are a large company, a SME or a citizen trying to complete an electronic transaction in another EU country, e.g. submit a call for tender or register as a student in another EU Member State (MS), besides reducing time and costs, the eIDAS Regulation will ensure cross border recognition of notified national eID mean and qualified trust services supporting your electronic transaction. Hence it will boost trust, security and convenience.

Since 1 July 2016, most provisions of the eIDAS Regulation are directly applicable in the 28 EU Member States' legal framework overcoming problems of fragmented national regimes. It provides legal certainty and fosters the usage of eID means and trust services for online access and online transactions at EU level.

The eIDAS Regulation will ensure that people and businesses can use their national eIDs to access public services in other EU countries where eIDs are required for such an access at national level. It also creates an EU wide internal market for qualified trust services by ensuring their recognition and workability across borders and considering them equivalent to traditional paper based processes.

1.2 Opportunities brought by the eIDAS Regulation

The opportunities reside in leveraging eID and electronic trust services as key enablers for making national and cross-border electronic transactions more secure, more convenient, trustworthy and benefiting from legal certainty.

The broader adoption of EU-wide recognised eID means and of electronic trust services will facilitate and boost the digital transformation of organisations, be it public administrations or businesses, enhance customer experience, improve the security of electronic transactions and stimulate the provisioning of new and innovative services.

To this end, a large number of sectors (e.g. finance, banking, transport, insurance, health, sharing economy, trading, etc.) where obligations exist for security, reliable identification, strong authentication and legal certainty of evidences, will be positively affected. The eIDAS Regulation will indeed allow citizens, businesses and public administrations to conveniently meet such obligations for any cross-border electronic transaction using the recognised eID means and (qualified) trust services of their choice.

[1] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[2] See Glossary or Art.3.16 of the eIDAS Regulation for the definition of trust services.

Without undergoing identity verification based on physical presence, but by using MS notified eID means of a level "high", one should for example be able to use public services in another country or banks may accept such eID to open a bank account[3]. By relying on a qualified electronic registered delivery service, one will benefit, all over the EU, from the presumption of the integrity of the registered data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by that qualified trust service.

1.3 Specific role of the qualified trust services

To further enhance in particular 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, the eIDAS Regulation introduces the notions of qualified trust service and qualified trust service provider with a view to indicating requirements and obligations that ensure high-level security of whatever qualified trust service or product is used or provided and, as a consequence, are granted a higher presumption of their legal effect.

Therefore, when looking for trust services, selecting qualified ones ensures benefiting from a high level of security and legal certainty of trust services. E.g., qualified electronic time stamp shall enjoy, all over the EU, the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

1.4 Initiation and supervision of qualified trust services

In order to ensure high-level security of qualified trust services, the eIDAS Regulation foresees an active supervision scheme of qualified trust service providers (QTSP) and the qualified trust services (QTS) they provide (hereafter referred to as a QTSP/QTS) by the national competent supervisory body (SB) that supervises, ex ante and ex post, fulfilment of the **QTSP/QTS requirements and obligations**. All those requirements must be met by the QTSP/QTS before providing the very first qualified trust service output, e.g. before issuing the very first qualified time stamp in the case of QTSP providing qualified time stamping services.

Before a TSP/TS is granted a qualified status (QTSP/QTS), it will be subject to a pre-authorisation process – the so called initiation process. QTSPs may only begin to provide the qualified trust service after the qualified status has been granted by the competent supervisory body and indicated in the national **trusted list**. From there, the supervision scheme covers the full life cycle of each QTS and each QTSP, from its genesis until its termination.

In practice, where TSPs, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by an "eIDAS" accredited conformity assessment body. Before notifying the competent supervisory body of their intention to start providing qualified trust services, the future QTSP/QTS must hence successfully pass an external assessment (audit) to confirm it fulfils the eIDAS requirements. That audit must be conducted by a conformity assessment body specifically accredited to carry out assessments of QTSP/QTS. The audit results in a formal conformity statement confirming - if such is the case - that the QTSP/QTS meets all the applicable requirements of the eIDAS Regulation. Based on the notified information including the report of such an audit, the competent SB will formally verify that

[3] National legislations on prevention of money laundering may currently may force identity verification to be based on physical presence. Furthermore, the use by the private sector of electronic identification means under a notified scheme is on a voluntarily basis only (see Recital 17 of the eIDAS Regulation).

the candidate QTSP/QTS meets the applicable eIDAS requirements and, in case of positive verification, it will undertake the publication of the grant of the qualified status for that QTSP/QTS in the national trusted list.

It is only when its qualified status is published in the corresponding national trusted list that the QTSP/QTS is authorised to provide the corresponding QTS.[4]

> Note: A TSP cannot be qualified without providing at least one qualified trust service (Art.3.20 of the eIDAS Regulation). A TSP is granted a qualified status separately for each type of qualified trust service covered by the eIDAS Regulation. E.g. a QTSP qualified for the provisioning of qualified certificates for electronic signatures is not per se granted a qualified status for the issuance of qualified electronic time stamps; it must first complete the full pre-authorisation process and have its qualified status granted for the creation of qualified electronic time stamps published explicitly in the national trusted list before issuing qualified time stamps in addition to the creation of qualified certificates for electronic signatures. There are nine different types of QTSs defined by the eIDAS Regulation for which a qualified status is granted separately: creation of qualified certificates for electronic signatures; creation of qualified certificates for electronic seals, creation of qualified certificates for website authentication, qualified preservation service for qualified electronic signatures, qualified preservation service for qualified electronic seals, qualified validation service for qualified electronic signatures, qualified validation service for qualified electronic seals, qualified electronic time stamps services, and qualified electronic registered delivery services.[5]
>
> Moreover, for a given type of QTS, if a QTSP has already been granted a qualified status for the provision of one or more such trust services intends to provide another QTS of the same type but under significantly different practices and/or policies, then it may be required to pass an ad hoc or complete conformity assessment before been confirmed a qualified status for that new way to provide such a QTS (Art. 24.2.(a), Art.20.2).

For marketing purposes, once qualified, a QTSP/QTS may use the EU Trust Mark for qualified trust services when promoting its QTS. That trust mark shown in Figure 1 can only be used by a QTSP to "label" its QTS. It can be used on any support provided it meets requirements from Art.23 of the eIDAS Regulation (e.g. a link to the corresponding national trusted list where consumers may verify the granted qualified status must be displayed on the QTSP's website) and rules of Commission Implementing Regulation (EU) 2015/806.[6] Basically, this secondary legislation sets the form, colour and size of the EU trust mark, sets the obligation to clearly indicate the qualified service that the EU trust mark pertains to, and allows association with other graphical or textual elements provided that certain conditions are met.[7]

---

[4] The eIDAS Regulation foresees transitional measures (Art.51) that ensures certification-service-provider issuing qualified certificates to natural persons under Directive 1999/93/EC to be considered as QTSPs issuing certificates for electronic signatures under the Regulation until they submit a conformity assessment report and the completion of its assessment by the supervisory body. The submission of that report shall not occur later the 1 July 2017 otherwise the CSP shall not be considered as a QTSP from 2 July 2017.

[5] See Annex A.7 for further details.

[6] Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (Text with EEA relevance). OJ L 128, 23.5.2015, p. 13–15.

[7] See https://ec.europa.eu/digital-single-market/en/news/eu-trust-mark for more guidance on the use of that trust mark, downloadable images, user manual and answers to frequently asked questions.

Figure 1 EU trust mark for qualified trust services

The use of the EU trust mark, which is voluntary, aims to foster transparency of the market and help consumers distinguishing between qualified trust services and non-qualified ones. Although based on self-assessment, it gives the assurance that the trust service providers and the trust services provided by them are qualified and comply with the rules set out in the eIDAS Regulation, thus ensuring a high quality which is regulated throughout the EU.

Once granted a qualified status, QTSPs and their QTSs have the obligation to pass, and submit to the competent supervisory body a conformity assessment report (CAR) issued by an accredited CAB confirming at least every 24 months, that the QTSP and the QTSs it provides fulfil the requirements laid down in the Regulation. Competent supervisory bodies are also allowed, at their own discretion and at any time, to audit themselves any QTSP/QTS for which they are competent or to request an accredited CAB to perform an ad hoc audit.

QTSPs and their QTSs are supervised for their entire lifecycle, from their genesis to their termination. In particular, in order to ensure sustainability and durability of QTSs, as well as to ensure proper termination and user's confidence in their provision, QTSPs must maintain, at all times, an up-to-date termination plan. That plan is to be agreed by the SB upon initiation and regularly checked for compliance during the life of the QTSP/QTS.

1.5 Scope of the present document and relationship with other recommendations

This document is one deliverable out of a series whose objective is to propose guidelines aimed at facilitating the implementation of the provisions related to trust services of the eIDAS Regulation in the area of qualified trust services[8].

This document proposes guidelines on the initiation of qualified trust services pursuant to Art.21.1 of the eIDAS Regulation. It should be read together with the "Guidelines on Supervision of Qualified Trust Services"[9].

The target audience of the document are trust service providers (including individuals, businesses and public administrations) who intend to start providing qualified trust services, those Member States supervisory bodies designated to carry out supervisory activities under the eIDAS Regulation, and conformity assessment bodies.

The objective of the document is to support TSPs intending to provide qualified trust services and supervisory bodies in their respective tasks and duties during the preparation phase, the notification phase, the initial verification of compliance with the eIDAS Regulation and the effective grant of the qualified status through the publication of an updated national trusted list. The guidelines cover the procedures and formats for initiating a qualified trust service. The guidelines shall enable supervisory bodies to clarify the rules, requirements and recommendations for a TSP to notify its intention to start

[8] https://www.enisa.europa.eu/topics/trust-services/guidelines/
[9] See the above footnote.

providing qualified trust services. The guidelines for the notifying TSPs aim to facilitate the implementation of the preparation of the provision of their qualified trust services and the notification phase of the initiation process as foreseen by the eIDAS Regulation.

The present document is organised to provide information and guidance with regards to:

- The provision of recommendations and guidelines to Supervisory Bodies and to Trust Service Providers (section 2).
- The eIDAS Regulation provisions related to the initiation of Qualified Trust Services (section 3).
- The initiation and supervision activities, process flow as well as the accreditation of CABs in accordance with the eIDAS Regulation (section 4).
- The format and procedure for notification under Art.21.1 of the eIDAS Regulation (section 5).
- The initial verification of the notified QTSP/QTS with the eIDAS requirements & communication of the granted qualified status for inclusion in the national TL (section 6).
- The Supervisory Body resources and organisational measures (section 7).

2. Guidelines on the Initiation of Qualified Trust Services

2.1 Introduction

The eIDAS Regulation sets the principle of non-discrimination of the legal effects and admissibility of electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and electronic documents as evidence in legal proceedings. Courts (or other bodies in charge of legal proceedings) cannot discard them as evidence only because they are electronic but have to assess these electronic tools in the same way they would do for their paper equivalent.

To further enhance in particular 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, the eIDAS Regulation introduces the notions of **qualified trust service** and **qualified trust service provider** with a view to indicating requirements and obligations that ensure high-level security and a higher presumption of their legal effect.

In order to ensure high-level security of qualified trust services, the eIDAS Regulation foresees an active supervision scheme of qualified trust service providers (QTSP) and the qualified trust services (QTS) they provide (hereafter referred to as a QTSP/QTS) by the national competent supervisory body (SB) that supervises, ex ante and ex post, fulfilment of the **QTSP/QTS requirements and obligations**.

Before a TSP/TS is granted a qualified status (QTSP/QTS), it will be subject to a pre-authorisation process – the so called initiation process. QTSPs may only begin to provide the qualified trust service after the qualified status has been granted by the national supervisory body and indicated in the national **trusted list**[2]. From there, the supervision scheme covers the full life cycle of each QTS and each QTSP, from its genesis until its termination.

2.2 Initiation of qualified trust services

In practice, the initiation process through which a TSP, without qualified status, that intends to start providing qualified trust services, is granted a qualified status is made of the following steps (see section 4 for a detailed analysis):

1. **Preparation**: The TSP designs, sets up, implements, tests and deploys in pre-production the QTS it intends to provide, in line with the eIDAS requirements. In parallel, the TSP establishes the relevant documentation that will demonstrate its compliance with the eIDAS requirements. An "eIDAS" accredited conformity assessment body (CAB)[10] assesses the conformity of the TSP and the QTS it intends to provide with the eIDAS requirements. The conformity assessment report (CAR) must prove the compliance of the TSP and the QTS it intends to provide with the eIDAS requirements and not with standards. Standards might nevertheless be a tool used by TSPs to support the demonstration of their compliance with eIDAS.
2. **Notification**: The TSP notifies the SB its intention to become qualified together with the conformity assessment report (CAR) issued by the "eIDAS" accredited CAB.

[10] That assessment must be conducted by a CAB specifically accredited by a national accreditation body (NAB) under Regulation (EC) 765/2008 to carry out assessments of QTSP/QTS against the requirements of the eIDAS Regulation (Art.3.18).

3. **Initial verification of compliance**: The SB verifies whether or not the TSP and the QTS it intends to provide meet the requirements of the eIDAS Regulation in order to be granted a qualified status. Final decision is in the hands of the SB. The latter may rely upon the information provided as part of the notification procedure, including the conformity assessment report, but is equally entitled to request further information and may take a duly justified decision that goes against the conformity assessment report. In that case, as for all its decisions, the SB should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality. Upon positive verification by the SB that the TSP and the QTS it intends to provide meet the eIDAS requirements, the SB grants the qualified status to the TSP/TS and informs the body in charge of the national trusted list for the purpose of updating this list.
4. **Publication of the qualified status in the national trusted list**: Upon notification by the SB that the notifying TSP/TS has been granted a qualified status, the body in charge of the national trusted list updates the list accordingly.

It is only when its qualified status is published in the corresponding national trusted list that the QTSP is authorised to provide the corresponding QTS[11].

The following sections proposes guidelines[12] to SBs, TSPs, and CABs on initiation of qualified trust services pursuant to Art.21.1 of the eIDAS Regulation.

[11] The eIDAS Regulation foresees transitional measures (Art.51) that ensures certification-service-provider issuing qualified certificates to natural persons under Directive 1999/93/EC to be considered as QTSPs issuing certificates for electronic signatures under the Regulation until they submit a conformity assessment report and the completion of its assessment by the supervisory body. The submission of that report shall not occur later the 1 July 2017 otherwise the CSP shall not be considered as a QTSP from 2 July 2017.

[12] The use of specific verbs (SHALL, SHOULD and MAY) are used in accordance with the ETSI-guide, https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/AGuideToWritingWorldClassStandards.pdf

2.3 Recommendations for Supervisory Bodies

The following are **recommendations** for supervisory bodies in the context of the initiation of QTS:

SB.1 – Supervisory body resources

(a) Make sure to be given the necessary powers and adequate resources for the exercise of its tasks.
(b) Make sure to establish, document and maintain the necessary policies, processes and procedures for the realisation of the supervisory activities foreseen in the eIDAS Regulation, including those related to the management of the national trusted lists.
(c) To this extent, follow recommendations provided in section 6 of this document.

SB.2 – Preliminary interactions with prospective QTSPs

(a) In order to allow an efficient initiation process, as stressed by Recital (45) of the eIDAS Regulation, preliminary interactions between prospective QTSPs and the national SB body are encouraged with a view to facilitating the due diligence leading to the provisioning of QTSs.
(b) Besides CID (EU) 2015/1505 requirement[13] on the publication of specific information on the underlying supervision scheme, SBs should publicize information about the initiation process and in particular the notification format and procedure, as well as information on the subsequent supervision process.

SB.3 – Format and procedure for notification under Art.21.1 of the eIDAS Regulation

(a) Make sure that the specifications and requirements on the format and procedure for notification under Art.21.1 of the eIDAS Regulation are properly communicated to the candidate TSPs and made available to the public.
(b) Follow recommendations provided in section 4 of this document on format and procedure for notification.

SB.4 – Confidentiality between SB and notifying (Q)TSP

(a) Unless already available in the public domain, the SB should limit disclosure of information/documentation provided by notifying (Q)TSP within its own organisation, to its directors, officers, members and/or employees having a need to know. Unless otherwise foreseen by European or national laws, and in particular the eIDAS Regulation, the SB shall not disclose such information/documentation to any third party.

SB.5 – "eIDAS" accreditation scheme for CABs

(a) Interactions are encouraged between the SB and the local national accreditation body (NAB), and where applicable the foreign NAB having accredited CAB selected by the TSP notifying its intention to provide QTS or candidate for such a notification, with a view to facilitating the verification of correct accreditation of the CAB selected by the notifying TSP to carry its assessment and the assessment of the notified QTS against the requirements of the eIDAS Regulation.

[13] See Annex I, Chapter II, Scheme information URI (clause 5.3.7) of 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 the eIDAS Regulation.

(b) Make sure that information about the accredited CABs and the underlying eIDAS accreditation scheme is available from the NAB website and communicated/notified to the EC (or the body designated to centralise such information if any).
(c) Make sure to consider as eligible and equivalent all CABs accredited by any NAB signatory of the European co-operation for Accreditation (EA) Multilateral Agreement (MLA) and all CARs delivered by them provided they are accredited in accordance with the eIDAS Regulation (Art.3.18, Art.20.1). Consider any CAB or CAR as non-eligible when this is not the case. See section 3.4 of this document for further guidance.

SB.6 – QTSP/QTS audit criteria & the structure of the initiation CAR

(a) Both for conducting Art.21 initial verification and for verifying the eligibility of CABs and CARs notified under Art.21.1, make sure that QTSP/QTS are assessed for compliance against each and every applicable requirement of the eIDAS Regulation.
(b) Make sure and verify that the CAR explicitly confirms and bears sufficient information demonstrating that the assessed QTSP/QTS fulfil the requirements of the eIDAS Regulation.
(c) Follow recommendations of section 4.5 of this document with regards to the recommended structure and content of CARs.

SB.7 – Initial verification of the notified QTSP/QTS with the eIDAS requirements

(a) Make sure that the notifying TSP fulfils the requirements on the format and procedure for notification under Art.21.1 of the eIDAS Regulation and that the QTSP/QTS are assessed for compliance against each and every applicable requirement of the eIDAS Regulation.
(b) Follow recommendations provided in section 6 of this document when conducting initial verification.

SB.8 – Communication of the granted qualified status and inclusion in the national trusted list

(a) The SB and the TLSO shall conform to CID 2015/1505/EU. See section 2.4 of this document for guidance on the granularity of the qualified status assignment.
(b) In particular, the SB and the TLSO shall respect the timing constraints clarified by this CID (enforcing clause 5.5.5 of ETSI TS 119 612 v2.1.1) making sure that the date, indicated in the corresponding national trusted list, of the grant of the qualified status, the date of signing of the trusted list and the effective date of publication of that trusted list are all aligned to the same date and that no back dating is allowed.

SB.9 – Cooperation with other EU MS SBs

(a) It is recommended that SBs cooperate to the specification of one (or a limited set) of eIDAS compliant conformity assessment scheme(s) once a sufficient maturity has been reached in the effective implementation and use of those schemes by accredited CABs to assess QTSP/QTS and by NABs to accredit CABs in accordance with eIDAS Regulation. The standardisation of such scheme(s) would later open the doors to a potential referencing in eIDAS implementing acts foreseen in Art.20.4.
(b) It is recommended to SBs to cooperate under Art.18 of the eIDAS Regulation to set-up a single and centralised dissemination point providing to the public, information, and any change thereto, about each of the EA MLA signatory NABs, whether they operate an accreditation scheme in accordance with the eIDAS Regulation, details regarding such an accreditation scheme, accredited

CABs and for which QTPS/QTS, accredited CABs conformity assessment activities (e.g. certification certificates), etc.

(c) Cooperation under Art.18 with other EU MS SBs is strongly recommended when notifying TSP activities and operations related to the provision of notified QTS are spread across national borders. See companion document "guidelines for supervision of qualified trust service providers" for further guidelines on such cooperation.

SB.10 – Good administration principles

(a) With regards to their activities, SBs should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality.

2.4 Recommendations for Trust Service Providers

The following are **recommendations** for trust service providers in the context of the initiation of QTS:

TSP.1 – Preparation to the provision of QTS as a QTSP

(a) Where TSPs, without qualified status, intend to start providing QTSs, they should design and test the organisational, physical and technical implementation of those trust services, as well as their corresponding practices, policies, procedures, processes and documentation in line with the requirements laid down in the eIDAS Regulation.

(b) For that purpose, TSPs should first consider the publication by the competent SB of the specifications and requirements on the format and procedure for notification under Art.21.1 of the eIDAS Regulation. In particular, they should organise their preparation for compliance with the requirements laid down in the eIDAS Regulation in line with the specifications and recommendations or requirements from the competent SB on the content and structure of the CAR they need to obtain from an eIDAS accredited CAB. See section 3.5 of this document for further details on the recommended structure of an eIDAS CAR.

(c) TSPs can select any CAB accredited in any EU MS provided the CAB has been accredited in accordance with Art.3.18 of the eIDAS Regulation (see section 0 of this document for further guidance). Before contracting any such CAB, TSPs should however make sure that the candidate CAB and the CAR it will issue in case of positive assessment will meet the expectations or requirements of the eIDAS Regulation and of the competent SB. In particular they shall make sure that the CAR shall confirm the compliance of the assessed QTSP/QTS with the requirements of the eIDAS Regulation (e.g. and not with whatever standard; the CAR may however confirm compliance to any set of standards in addition to confirming that the eIDAS requirements are fulfilled but the main purpose of CAR submitted to the SB under Art.21.1 of the eIDAS Regulation shall be to confirm that the assessed QTSP/QTS fulfil the requirements laid down in the eIDAS Regulation).

(d) Appropriate preliminary interactions with the national SB is recommended.

(e) Standards and normative documents may be of great help to ensure best practices are followed and to maximise interoperability of the implemented services. Specific standards having been designed aiming to enable compliant implementation meeting the eIDAS Regulation requirements. ETSI TR 119 000[14] is the overview document to obtain information on which CEN or ETSI standards

[14] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

that may be considered when implementing a specific type of (qualified) trust service. It should be made clear nevertheless that it is not mandatory and it cannot be made mandatory to comply with any standard. No standard, at the date of publication of this document has yet been formally assessed as meeting QTSP/QTS requirements of the eIDAS Regulation. Furthermore ENISA published an analysis of standards related to TSPs, mapping the eIDAS requirements to existing standards[15]. It concluded that the analysed standards usually cover some requirements in part or whole but also led, however, to a shortlist of gaps where specific eIDAS requirements have yet to be addressed in EU standards (ETSI/CEN/CENELEC) or international ones.

(f) When notifying TSPs intend to provide QTS so that it meets requirements from another application domain, provided they are not in contradiction with the eIDAS requirements, they may be required to comply with specific standards or normative requirements. For example, QTSP providing services consisting in the issuance of qualified certificates for website authentication (QWACs) may be required to meet specific standards to meet the CA/Browser Forum requirements and requirements from Browsers or widely deployed applications owners[16]. (Q)TSPs willing to benefit from recognition in both eIDAS and non-eIDAS worlds (e.g. CA/Browser Forum) should ensure that the conformity assessments they pass to demonstrate compliance with the eIDAS requirements can be of benefit in the demonstration of their compliance with those non-eIDAS requirements and that those requirements and their implementation by the (Q)TSP are not in contradiction with the eIDAS Regulation.

(g) In addition to any applicable national language, all relevant (Q)TSP/(Q)TS documentation should be made available in UK English in order to facilitate cross-border provision of services.

TSP.2 – Notification of the intention to provide QTS as a QTSP

(a) Where TSPs, without qualified status, intend to start providing QTSs, they need to submit to the SB a notification of their intention together with a CAR issued by a CAB.

(b) For that purpose, they have to meet the specifications and recommendations or requirements from the competent SB on the content and structure of the CAR they need to obtain from an accredited CAB.

(c) See section 4 of this document for guidance on format and procedure for notification.

TSP.3 – Understanding the granularity of the identification of a trust service to which a qualified status is granted

(a) TSPs and QTSPs should understand the granularity of the identification of a trust service to which a qualified status is granted, as discussed in section 3.4 of this document, to identify when they are required to notify the initiation of a new QTS and when they actually need to notify any change to an existing QTS or that existing service being subject to routine supervision and 2-yearly audits.

TSP.4 – Preliminary interactions with competent SB

[15] https://www.enisa.europa.eu/publications/tsp_standards_2015/at_download/fullReport.

[16] Users of compliant QTSPs will then benefit from the recognition by CA/Browser Forum member's applications such as Internet browser software that will then display enhanced indication of the corresponding certified website identity by changing the appearance of its display (i.e. colours, icons, animation, and/or additional website information) to reflect its trustworthiness.

(a) In order to allow an efficient initiation process, as stressed by Recital (45) of the eIDAS Regulation, preliminary interactions between prospective QTSPs and the national SB are encouraged with a view to facilitating the due diligence leading to the provisioning of QTSs.

2.5 Recommendations for Conformity Assessment Bodies

The following are **recommendations** for CABs in the context of the assessment of (Q)TSP/(Q)TS:

CAB.1 – eIDAS accreditation requirements for CABs assessing a QTSP/QTS

Make sure to be properly accredited in accordance with the requirements of the eIDAS Regulation. In particular:

- Art.3.18 of the eIDAS Regulation requires CABs to be accredited in accordance with Regulation (EC) No 765/2008 in a way that such accreditation ensures the accredited CABs are competent to carry out conformity assessment of a QTSP/QTS against the requirements of the eIDAS Regulation.
- The resulting conformity assessment report to be submitted to the supervisory body by the assessed (Q)TSP, whether in the context of a 2-yearly regular audit (Art.20.1), an ad hoc audit (Art.20.2) or an initiation audit (Art.21.1) must be such that it confirms, when this is the case, that the assessed (Q)TSP/(Q)TS fulfil all the applicable QTSP/QTS requirements of the eIDAS Regulation.
- The conformity assessment scheme (including requirements on the CAB, requirements on the auditing rules under which the CAB will carry out their conformity assessment and the effective set of criteria, control objectives and controls against which it will assess a QTSP/QTS with the aim of confirming that it fulfils the eIDAS requirements) may be defined by the CAB itself, the EU MS supervisory body, or any other body possessing the necessary technical competence.

CAB.2 – Structure of eIDAS CAR

Follow recommendations provided in section 4.5 of this document.

CAB.3 – Preliminary interactions with national SBs

In order to facilitate evaluation of CARs notified under the eIDAS Regulation and the evaluation of (Q)TSP/(Q)TS by the SB of the EU MS in which CABs are active, preliminary interactions between CABs and those SBs are encouraged.

3. eIDAS Regulation provisions related to the initiation of qualified trust services

3.1 Supervisory bodies

Art. 17 of the eIDAS Regulation requires EU MS to designate a supervisory body established in their territory (or, upon mutual agreement with another Member State, a supervisory body established in that other Member State) to be responsible for supervisory tasks in their territory. Each EU MS is further required to give such a body the necessary powers and adequate resources for the exercise of those supervisory tasks (see Art.17.4 of the eIDAS Regulation).

3.2 QTSP/QTS initiation

The legal obligations related to the initiation of QTSPs/QTSs are mainly derived from Art.21 of the eIDAS Regulation as listed here after:

- *Art.21.1. - Where trust service providers, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by a conformity assessment body.*
- *Art.21.2. - The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.*

  If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

  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.
- *Art.21.3. - Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).*

Recital (45) of the eIDAS Regulation also states that "*in order to allow an efficient initiation process, which should lead to the inclusion of qualified trust service providers and the qualified trust services they provide into trusted lists, preliminary interactions between prospective qualified trust service providers and the competent supervisory body should be encouraged with a view to facilitating the due diligence leading to the provisioning of qualified trust services*".

3.3 CABs and CARs

The conformity assessment body (CAB) and the conformity assessment report (CAR) referred to in Art.21.1 are further specified by or further specifications can be derived from the following:

- Art.3.(18) defines a 'conformity assessment body' as *a body defined in point 13 of Article 2 of* Regulation (EC) No 765/2008,[17,18] *which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides*.
- Regulation (EC) No 765/2008, Art.2.(13) defines:
  - a 'conformity assessment body' as *a body that performs conformity assessment activities including calibration, testing, certification and inspection",*
  - a 'conformity assessment' as *the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled,*
  - 'accreditation' as *an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity*;
  - a 'national accreditation body' as *the sole body in a Member State that performs accreditation with authority derived from the State*.
- Art.20.1 of the eIDAS Regulation requires that *the purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation.* Consequently, the resulting conformity assessment report needs to include a formal conformity statement confirming, when applicable, that the audited QTSP/QTS meets all the applicable requirements of the eIDAS Regulation.

The Commission did not adopt any implementing act with regards to the supervision of qualified trust services providers (Art.20.4) or the initiation of qualified trust services (Art.21.4).

Neither the business nor the technical model can be imposed upon the QTSPs nor a specific standard to be followed for the QTS it provides. (Q)TSP/(Q)TS have to demonstrate their compliance (building upon standards if it deems it appropriate) with the requirements of the eIDAS Regulation while the supervisory body cannot refuse to grant the qualified status solely on the grounds that the proposed model does not comply with a given standard or a given business/technical model. QTSP/QTS are free to define the way to proceed to the implementation of the eIDAS applicable requirements, whether operationally, organisationally or technically.

3.4 Granularity of qualified status assignment

The present section discusses the granularity of the assignment of a qualified status to a QTSP/QTS, both in the context of the related information appearing in the national trusted list and its impacts on the need to process to the Art.21.1 initiation or to the Art.24.2.(a) notification of change in case of any change in the provision of a QTS.

A TSP cannot be deemed to be of a qualified level without providing at least one qualified trust service (Art.3.20 of the eIDAS Regulation). The qualified status is granted both to a TSP and to the trust service it provides when it has been included in the corresponding national trusted list after it has been verified by the competent supervisory body (SB) that both the TSP and the trust services provided by it (TSP/TS) comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified

[17] 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 (Text with EEA relevance). OJ L 218, 13.8.2008, p. 30–47.
[18] See Annex A.5 for what Regulation (EC) 765/2008 brings as advantages to SBs and to TSPs.

trust service providers and for the qualified trust services they provide (for QTSP/QTS). A TSP is granted a qualified status separately for each type of qualified trust service covered by the eIDAS Regulation. The granularity in terms of what QTS may exist in the sense of this Regulation is limited to that closed list of QTS for which there are applicable requirements in the Regulation (see Annex A.7).

> Example: A TSP that is granted a qualified status for the provision of a service providing qualified certificates for electronic signatures is not to be considered as qualified for the provision of any other qualified trust service, including the provision of qualified certificates for electronic seals or for website authentication, the provision of qualified electronic time stamps, etc., unless it has been granted a qualified status for such other QTS.

The granularity of the identification in the national trusted lists of the technical instance of the eIDAS qualified trust service to which the qualified status is granted is actually clarified by Commission Implementing Decision (EU) 2015/1505[19]. It corresponds to the level of the "Service digital identity" field as specified in ETSI TS 119 612 v2.1.1 on which the CID relies to establish the content and define the technical specifications and formats for the national trusted lists. In a trusted list, a qualified trust service to which a qualified status is granted is identified by the public key[20] identified by the "Service digital identity" field of the corresponding trusted list service entry of a listed TSP entry. The type of qualified trust service for which the qualified status is granted is identified by the combination of the "Service type identifier" field and the "additional Service Information" service information extension when present and further specifying the type of service[21].

When based on public key infrastructure (PKI) public key-technology, the public key referring to the "Service digital identity" field can be associated:

- either with the technical unit that is directly issuing, under the name of the listed TSP, the qualified trust service output (e.g. a qualified certificate for electronic signature, a qualified time stamp, a qualified electronic delivery evidence, a qualified validation result report on the qualified validation of a qualified electronic seal, etc.),
- or with a technical unit that is issuing digital certificates to one or more technical units that in turn are directly issuing the qualified trust service output under the name of the listed TSP or from which a certification path can be established "down to" one or more technical units that are issuing the qualified trust service output under the name of the listed TSP.

On one hand, to the level of information provided in the trusted list, it is the public key referring to the value of the "Service digital identity" field that will delimit the boundaries of the so-identified trust service to which the qualified status is indicated as "granted"[22] in the corresponding "Service current status" field (or "Service previous status" as part of the service status history), irrespective of the fact that a "commercial" qualified

[19] 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 (Text with EEA relevance). OJ L 235, 9.9.2015, p. 26–36.

[20] When based on PKI public-key technology (when not based on such technology, an indicator expressed as a URI is used to identify uniquely and unambiguously the listed service).

[21] See clauses 5.5.1 and 5.5.9.4 of ETSI TS 119 612 v2.1.1 on which CID (EU) 2015/1505 relies to lay down technical specifications and formats relating to national trusted lists.

[22] The corresponding identifier expressed as a URI to indicate such grant of a qualified status is http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted.

trust service provided by a QTSP may make use of several technical units directly issuing the corresponding qualified trust service outputs[23].

On the other hand, the initiation process foreseen by Art.21 of the eIDAS Regulation is required to be undergone by a TSP not having already a qualified status for the provision of a specific type of QTS. In that case it must submit to the supervisory body a notification of its intention together with a conformity assessment report issued by a conformity assessment body. That eIDAS article is however not applicable to TSPs being granted a qualified status for the same type of qualified trust service. In case of any change in the provision of its qualified trust services (incl. affecting existing listed technical units to which the grant of the qualified status is indicated, or when adding or removing technical units as part of the technical implementation of the qualified trust service), Art.24.2.(a) applies to the QTSP, which is required to notify the supervisory body of any change in the provision of its qualified trust services. It will then be up to the supervisory body to assess the impact of the notified changes on the need to undertake ad hoc audits or to request a conformity assessment body to perform a conformity assessment of the QTSP, at the expense of the QTSP, to confirm that the QTSP/QTS fulfils the requirements laid down in this Regulation (Art.17, Art.20.2). In line with Art.20.3, it is possible for the supervisory body to withdraw the qualified status of the concerned qualified trust services, in practice to the level of granularity of the identification in the national trusted lists of the technical instance of the concerned qualified trust service to which the qualified status is granted.

The above must however be nuanced with regards to the CSPs issuing qualified certificates to natural persons and migrated as QTSP issuing qualified certificates for electronic signatures under Art.51.3 of the eIDAS Regulation. For those QTSPs, any change that "significantly" deviates from the provision of the corresponding services as they implemented them before the 1st of July 2016, requires them to go through the Art.21.1 initiation process as, in that case, they would break the conditions of applicability of the transitional measures. E.g. a former CSP issuing qualified certificates to natural persons under Directive 1999/93/EC, creating a new issuing CA and/or root CA (compared to the existing listed qualified trust service corresponding entries in the national trusted list) under different practices[24] resulting from significant changes compared to the one they implemented under the Directive (e.g. in order to be able to meet the eIDAS requirements), should go through Art.21.1 initiation process before being granted a qualified status for that new issuing CA/root CA. And if this concerns a qualified trust service already listed, it should be for that service as well that the CSP/QTSP must go through the Art.21.1 initiation process. However, such a former CSP only modifying the profile of its end-entity qualified certificates issued to natural persons (i.e. for electronic signatures) in order to meet requirements of Annex I of the eIDAS Regulation, without changing significantly anything else with regards to the provision of their services benefiting from the Art.51 measures should not need to go through Art.21.1 initiation process.

Of course, as said, in all cases of application of Art.24.2.(a), a "classification" of changes should in practice be considered, i.e. assessing how "significant" is the change and the impact it may have on the provision of the services to justify an ad hoc audit by the SB or by a CAB at the request of the SB under Art.20.2, the scope of such an audit.

Art.24.2.(a) of the eIDAS Regulation does not prevent notified changes to be already implemented before being notified by the QTSP to the supervisory body (on the contrary to the termination where the intention

[23] The pros and cons of listing either one or other option are discussed in ETSI TS 119 612 v2.1.1 for trust services involved in the issuance of digital certificates, i.e. either listing a Root CA or an issuing CA.
[24] With those "practices" to be understood as including all component services they may use and use differently, including service factory, devices, registration authorities, certificate validity status information services, etc.

to cease activities is required to be notified, hence, before cessation). Nevertheless, it is recommended to the QTSP to notify them before implementation so that the supervisory body could be able to approve (or make comments / indicate possible eIDAS non-conformities on) some significant changes before they are implemented.

Examples:

(i) When a TSP has been granted a qualified status, hence recognised as a QTSP, for the provision of qualified certificates for electronic signatures through a qualified trust service identified in the national trusted list by an issuing technical CA with public key X, whenever that TSP is willing to generate and operate a new technical issuing CA with public key Y, that TSP needs to notify the supervisory body of that change under Art.24.2.(a) for its inclusion in the trusted lists as a new entry as part of the entries related to the qualified trust service[25].

(ii) When that same QTSP later decides to implement changes in the provision of the qualified trust service affecting the issuing technical CA with public key X in a way that requires the supervisory body to withdraw the qualified status, this can be done at the level of the trusted list entry corresponding to the issuing technical CA with public key X. When the technical issuing CA with public key Y would be assessed by the supervisory body as not being impacted in that way, the SB may decide to keep the qualified status for that service as being granted.

(iii) A TSP is granted a qualified status for the provision of qualified certificates for electronic signatures through a qualified trust service identified in the national trusted list by a technical root CA with public key X, under which e.g. a large number of technical issuing CA are used to issue end-entity certificates:
    (a) Whenever that TSP modifies the sub-ordinate and issuing CA topology under the listed root CA, it needs to notify the supervisory body of such changes.
    (b) When adding or discarding technical CAs under the listed root CA, the QTSP needs to notify the supervisory body of such changes under Art.24.2.(a).

(iv) When a QTSP provides qualified certificates for electronic signatures through a qualified trust service identified in the national trusted list by an issuing technical CA with public key X, intends to use that same issuing technical CA with public key X to issue qualified certificates for electronic seals and/or for website authentication certificates, it must go through Art.21.1 initiation process when not already given a qualified status for the provision of such other type(s) of qualified certificates or when that would significantly change the provision of such other type(s) of qualified certificates for which it has already been given a qualified status. Otherwise that change needs to be notified to the supervisory body under Art.24.2.(a) for updating the national trusted list when assessment by the supervisory body would lead to such an update.

(v) When a TSP has been granted a qualified status, hence recognised as a QTSP, for the provision of qualified time stamps through a qualified trust service identified in the national trusted list by a technical CA issuing certificates to technical time stamping units (TSUs) that in turn will each issue qualified time stamps, then whenever that TSP will decide to create a new TSU certified by that listed CA, it will not need to go through Art.21.1 notification for being granted a qualified status for that service but will need to notify the competent supervisory body of that change regarding the listed qualified service as any change in the provision of its qualified service required to be notified as per Art.24.2.(a) of the eIDAS Regulation.

[25] Provisions of clause 5.5.5 of ETSI TS 119 612 v2.1.1 pursuant to CID (EU) 2015/1505 apply with regards to the allocation of the date to which such a change applies.

See also annex A.4 of this document for guidance on the use of "Service digital identity" field in trusted list with regards to qualified trust services.

3.5 Standards and best practices

As previously stated, neither the business nor the technical model can be imposed on QTSPs nor a specific standard to be followed for the QTS it provides. The ultimate goal of the conformity assessment report resulting from the assessment of a QTSP/QTS by a CAB accredited under Regulation (EC) 765/2008 is to confirm that the QTSP/QTS fulfils the requirements laid down in the eIDAS Regulation (Art.20.1) not that it complies with a specific standard.

Furthermore, no standard is referenced so far by any eIDAS secondary legislation for the presumption of compliance with all or parts of the eIDAS requirements applicable to QTSPs and the QTSs they provide.

However, standards developed or still under development by European standardisation organisations (ESOs) or other international standardisation organisations can be used to support:

- CABs, national accreditation bodies (NABs), and SBs in the establishment of the effective eIDAS QTSP/QTS criteria, the related control objectives, and the controls that will be used for assessing QTSP/QTS against the eIDAS Regulation;
- TSPs when designing, implementing and establishing their demonstration that they and the QTS they provide or intend to provide meet the applicable requirements of the eIDAS Regulation.

A formal assessment of a candidate standard of its compliance with the requirements set in the Regulation would in any case be required before its referencing to support the assessment of QTSP/QTS, ideally by the EC in the context of adopting related implementing acts pursuant to requirements of the eIDAS Regulation, or when this is not possible, by competent SBs, NABs, or CABs to build conformity assessment schemes aiming to assess conformity of QTSP/QTS with the eIDAS Regulation requirements.

Nevertheless, standards and normative documents may be of great help to ensure best practices are followed and to maximise interoperability of the implemented services. A supervisory body may establish an eIDAS conformity assessment scheme on the basis of referenced technical specifications or standards, with or without amendments after assessment of their compliance with the requirements set in the Regulation, so that once the criteria are met by the corresponding QTSP/QTS they may benefit from a presumption of compliance with the applicable eIDAS requirements with regards to the supervisory body decision pursuant to Art.21.2 of the eIDAS Regulation.

Specific standards have been designed by CEN and ETSI aiming to enable compliant implementations that meet the eIDAS Regulation requirements. ETSI TR 119 000[26] is the overview document to obtain information on which CEN or ETSI standards may be considered when implementing a specific type of (qualified) trust service. While those ETSI and CEN standards are not and cannot be mandatory for a QTSP/QTS to be followed, they have been developed as a means of best practice for a (Q)TSP to cover the eIDAS requirements. Moreover ENISA published an analysis of standards related to TSPs, mapping the eIDAS requirements to existing standards[27]. It concluded that the analysed standards usually cover some

[26] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".
[27] https://www.enisa.europa.eu/publications/tsp_standards_2015/at_download/fullReport

requirements in part or whole but it also led, however, to a shortlist of gaps, where specific eIDAS requirements have yet to be addressed in EU standards (ETSI/CEN/CENELEC) or international ones.

The eIDAS Regulation does not mandate compliance with any specific standard, and such compliance cannot be mandatory. However, it may be appropriate or even required for the notifying TSP intending to provide QTS to ensure that it complies with specific standards in order to satisfy requirements in another application domain, provided they are not in contradiction with the eIDAS requirements for QTSP/QTS. For example, QTSP providing services for the issuance of qualified certificates for website authentication (QWACs) may be required to meet specific standards to satisfy the CA/Browser Forum[28] requirements and requirements from Browsers or widely deployed applications owners for inclusion in their trusted certificate root stores. Users of compliant QTSPs will then benefit from the recognition by CA/Browser Forum members' applications such as Internet browser software that will then display enhanced indication of the corresponding certified website identity by changing their appearance (i.e. colours, icons, animation, and/or additional website information) to reflect its trustworthiness. Those (Q)TSPs willing to benefit from recognition in both eIDAS and non-eIDAS worlds (e.g. CA/Browser Forum) should ensure that the conformity assessments they pass to demonstrate compliance with the eIDAS requirements can be of benefit in the demonstration of their compliance with those non-eIDAS requirements. In the specific context of QWACs, ETSI EN 319 411 series has been designed to allow for such convergence of the eIDAS and CA/Browser Forum conformity assessments.

[28] The CA/Browser Forum is a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS and code signing and has established guidelines to provide greater assurance to Internet users about the web sites they visit by leveraging the capabilities of SSL/TLS certificates. See www.cabforum.org.

4. Initiation and supervision of QTSPs/QTSs

4.1 Initiation and supervision as corner stones of the eIDAS pyramid of trust

The ex-ante and ex-post model for the supervision of qualified trust service providers (QTSPs) and of the qualified trust services (QTSs) they provide is the foundation of the whole legal and trust model for such services as defined by the eIDAS Regulation. The eIDAS Regulation is actually setting up a complete pyramid of trust, which is illustrated in Figure 3.

The most visible part is the "EU trust mark for qualified trust services", which each qualified trust service provider may, on a voluntary basis, use to brand and promote the quality and trustworthiness of the qualified trust services it provides.

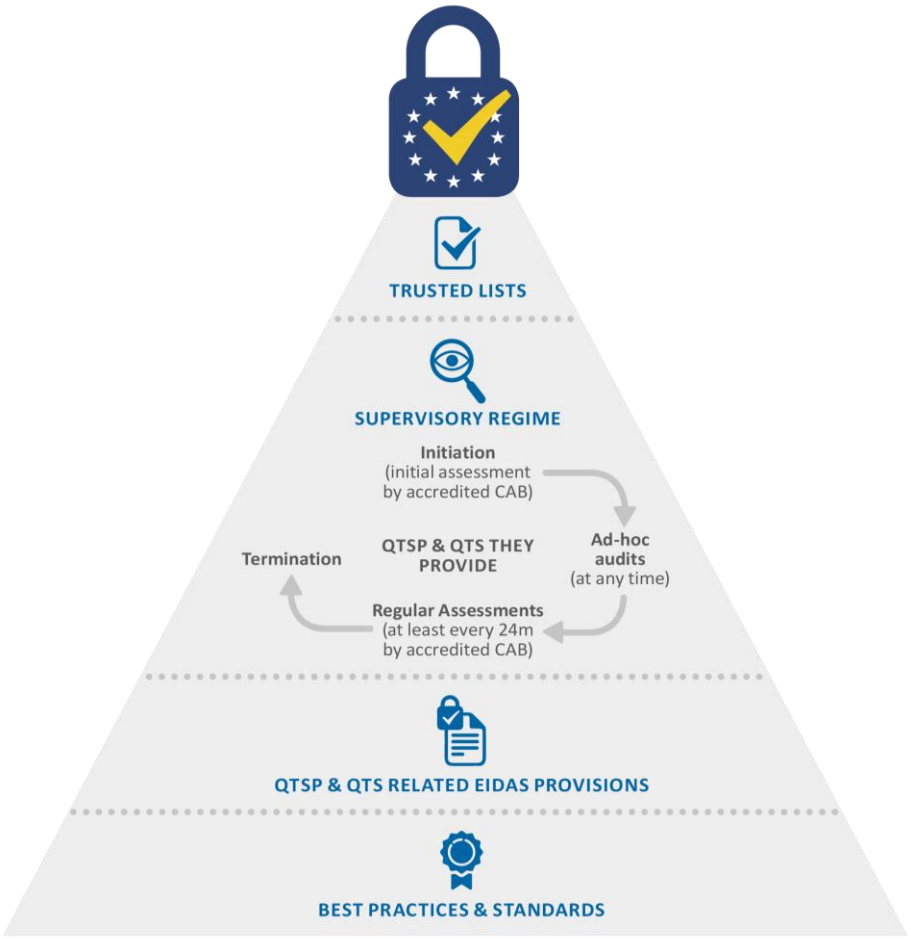

Figure 2 eIDAS Regulation building trust in the online environment (Source IAS² - updated)

This EU trust mark is not just another quality logo without any trust foundation (despite the fact that it's not verifiable in an automated way). As illustrated in Figure 2 above, the eIDAS Regulation explicitly sets up a consistent set of quality/security requirements and obligations for QTSPs/QTSs. Those requirements and obligations aim to enhance the trust of consumers and enterprises, in particular SMEs, in the internal (electronic) market and to promote the use of such QTSs and related products.

Through ex-ante and ex-post supervisory activities the eIDAS Regulation builds a supervisory regime upon those quality/security requirements and obligations for QTSs and QTSPs. It aims to ensure that, from genesis up to termination of such services, the QTSPs and the QTSs they provide indeed meet the requirements laid down in the Regulation.

This supervisory regime for QTSs and QTSPs is executed by each EU Member State (MS), by a national supervisory body, and follows common requirements to ensure a comparable security level of QTSs in all EU Member States (MS).

The supervisory regime covers the entire life-cycle of the QTSP and their QTSs:

- It relies on a pre-authorisation mechanism obliging trust service providers intending to provide QTSs to notify its nationally designated supervisory body of their intention together with a CAR issued by an accredited CAB confirming that the QTSP and the QTSs it intends to provide meet the requirements laid down in the Regulation.
- It obliges, once granted a qualified status, QTSPs to submit to the designated supervisory body, for each of their QTSs, a two-yearly conformity assessment report (CAR) issued by an accredited CAB confirming that the QTSP and the particular QTS it provides fulfil the requirements laid down in the Regulation.
- It allows designated supervisory bodies, at their own discretion and at any time, to audit a QTSP/QTS or to request an accredited CAB to carry out a conformity assessment of a QTSP/QTS and to produce a CAR confirming that it fulfils the requirements laid down in the Regulation.
- It foresees rules to be followed by QTSP and supervisory activities to be performed in cases where the QTSP changes or terminates the provisioning of a QTS, or ceases its activities.

The decisions to grant or withdraw a qualified status to trust services and trust service providers, resulting from the above supervisory activities, are taken by the designated national supervisory bodies.

Those status decisions are published on electronically signed or sealed national trusted lists. Such national trusted lists are established, maintained and published to disseminate in a trustworthy manner information related to the qualified trust service providers for which an EU MS is responsible, together with information related to the qualified trust services provided by them, including the whole history of the qualified status they have been granted.

The mandatory EU MS national trusted lists are published at least in a form suitable for automated processing. In practice these are XML files. The "*EU trust mark for qualified trust services*", despite the fact that its use by QTSPs is voluntary, is aimed to be the consumer visible means to convey the same information to the non-automated mass market. The eIDAS Regulation obliges QTSPs using such a trust mark to provide, close to it, a link to the corresponding trusted list allowing for verification.

The pyramid of trust in (qualified) trust services established by the eIDAS Regulation further relies on and is strengthened by the use of best practices and standards. In order to ensure uniform conditions for its implementation, the Regulation confers implementing powers on the Commission, for specifying implementation specifications or for referencing numbers of standards the use of which would raise a presumption of compliance with certain requirements laid down in the eIDAS Regulation (Recital (71)).

4.2 QTSP/QTS initiation and supervision activities

The various steps foreseen in the eIDAS Regulation regarding the initiation of a QTSP and of the QTS it provides and the related supervisory activities throughout the lifecycle of such services, from genesis until termination, can be depicted in the Figure 3.

In a nutshell, the **initiation** step consists in the following phases:

- The preparation.
- The notification.
- Initial compliance verification, including:
    - The analysis of the notification (procedure and format).
    - The analysis of the submitted conformity assessment report.
    - Granting, in case of positive verification, a qualified status to the TSP and to the trust service(s) they provide.
- Publication of the qualified status in the national trusted list.

Once qualified status is granted, the **life cycle management of the supervision** by the competent supervisory body to ensure that QTSPs/QTSs meet the requirements laid down in the Regulation can be split into several phases of related supervisory activities, as they are driven by the following events, each of which having the possibility to lead to a withdrawal of the qualified status:

- Regular (2-yearly) audits.
- Events monitored and detected by the SB.
- Termination of one, more or all of the qualified trust services.
- Other events notified by QTSPs:
    - Changes in the provision of a QTS.
    - Security breach.
    - Personal data breach.
    - Results of surveillance audits, when applicable.
- Other notified events, e.g.:
    - Complaints.
    - Request for cooperation from other SBs.

The present document covers the different phases of the initiation step listed above (“preparation”, “notification”, “initial compliance verification”, and “publication of the qualified status”). More specifically, it covers the procedures and formats for becoming a qualified trust service provider and for initiating a qualified trust service.

The companion deliverable of the present document (“Guidelines on Supervision of Qualified Trust Services”[29]) aims to provide recommendations to facilitate the implementation of the provisions related to qualified trust services of the eIDAS Regulation in the area of those phases related to the life cycle management of their supervision once they have been granted a qualified status.

[29] https://www.enisa.europa.eu/topics/trust-services/guidelines/.

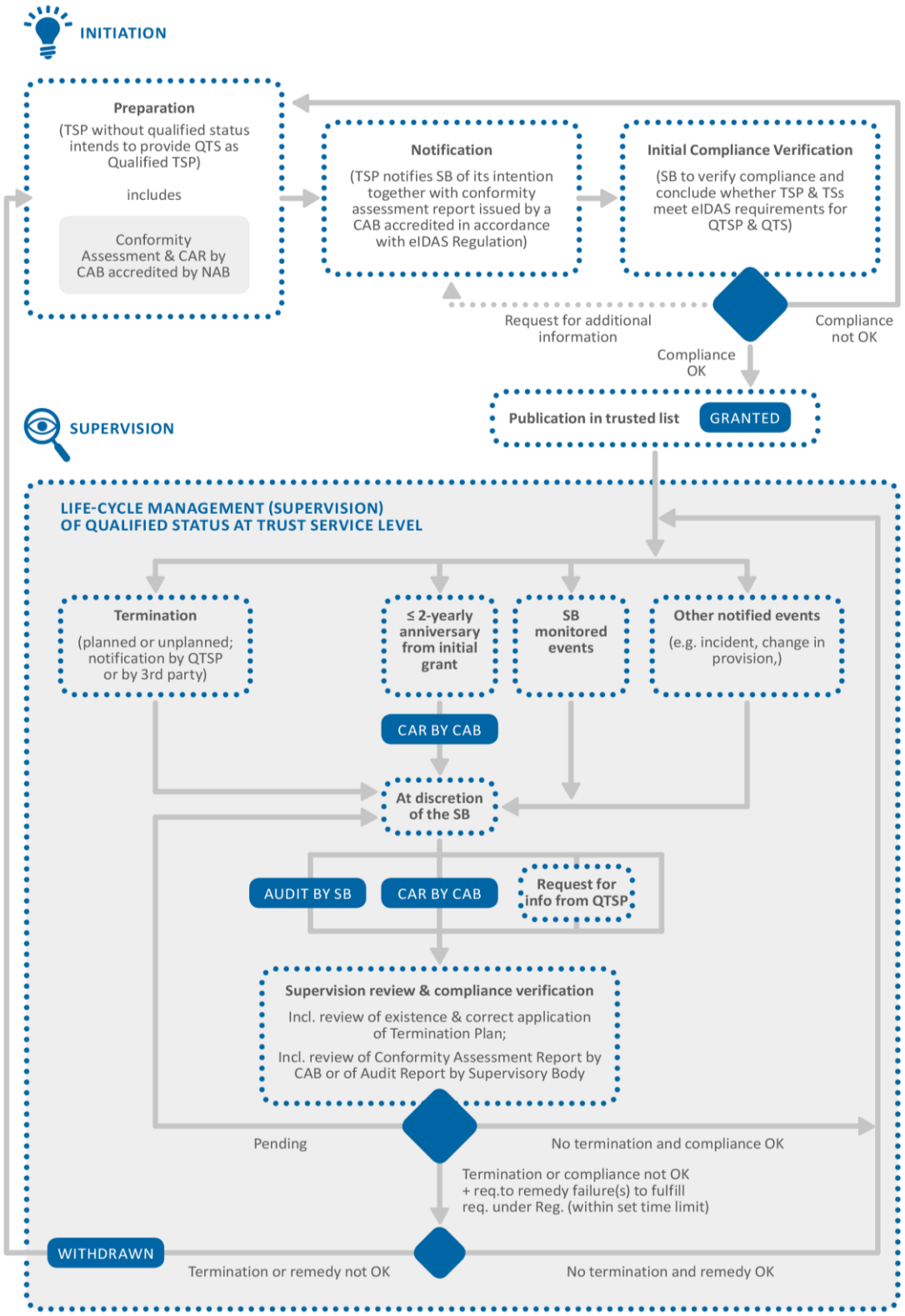

Figure 3 Overview of the QTSP/QTS initiation and life cycle management of the related qualified status at the trust service level and the related supervision activities. (Source IAS[2] - updated)

4.3 The initiation process flow

In order for a TSP/TS to be granted a qualified status, the TSP needs to go through the **initiation process**. This process must be executed for each specific type of QTS (as they are specified in the eIDAS Regulation) of which a TSP intends to start the provision, and for which the TSP has not already received a qualified status (see Art.3.20 and Art.21.1).

The process has also to take into account the level of granularity addressed in the national trusted list to correctly reflect the grant a qualified status to the TSP/TS when it passes the initiation process successfully and is granted such a qualified status.

The initiation process flow can be split into the following steps of related bodies' activities, as sketched in Figure 3 and detailed in Figure 4:

- The **preparation**: This step consists for the TSP intending to provide a qualified trust service.
    - **Design, set-up, implement, test and deploy the (qualified) trust service in pre-production** in line with the requirements laid down in the eIDAS Regulation. As the purpose of the initiation process will be to demonstrate its compliance to the eIDAS requirements and not to any standard, the TSP should build the provision of the QTS and document it in a way that facilitates the demonstration of its conformity with the eIDAS requirements. To this extent, best practices and standards when they are available may nevertheless be a tool used to facilitate such a demonstration.

    - **Setting-up the relevant documentation**: As said, the documentation related to the provision of the QTS should be established in a way to support and facilitate the demonstration of conformity to the eIDAS requirement. As prior to the verification by the national SB of the conformity of the notifying TSP/TS with the corresponding QTSP/QTS requirements of eIDAS, the TSP/TS will have to pass an audit by an accredited CAB, TSP should structure their documentation against the eIDAS requirements (see section 4.5 for further guidance). In a nutshell the documentation should include:
        - The risk assessment related documentation aimed to support demonstration of the requirement of Art.19.1.
        - A security & personal data breach notification plan aimed to support demonstration of the requirement of Art.19.2.
        - The termination plan (Art.24.2.(i)).
        - Declaration of practices, policies, security concept, procedures and guidelines the TSP will use to provide the QTS aimed to support demonstration of the other applicable eIDAS requirements.

    - **Conformity assessment**: That assessment must be conducted by a CAB specifically accredited by a national accreditation body under Regulation (EC) 765/2008 to carry out assessments of QTSP/QTS against the requirements of the eIDAS Regulation (Art.3.18).

- The **notification**: The TSP submits to the national SB the ad hoc notification form (as prescribed by the SB) together with the required documentation, when applicable and together with the conformity assessment report. That latter must prove the compliance with the requirements of the Regulation.

- The **initial compliance verification**: The SB verifies whether or not the TSP and the QTS it intends to provide meet the requirements of the Regulation in order to be granted the qualified status. Final decision is in the hands of the SB. The latter may rely upon the information provided as part of the

notification procedure, including the conformity assessment report, but is equally entitled to request further information and may take a duly justified decision that goes against the conformity assessment report. In that case, as for all its decisions, SB should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality. Upon positive verification by the SB that the TSP and the QTS it intends to provide meet the eIDAS requirements, the SB grants the qualified status to the TSP/TS and informs the body in charge of the national trusted list for the purpose of updating it.

- The **update of the trusted list**: Upon notification by the SB that the notifying TSP/TS has been granted a qualified status, the body in charge of the national trusted list updates the list accordingly.

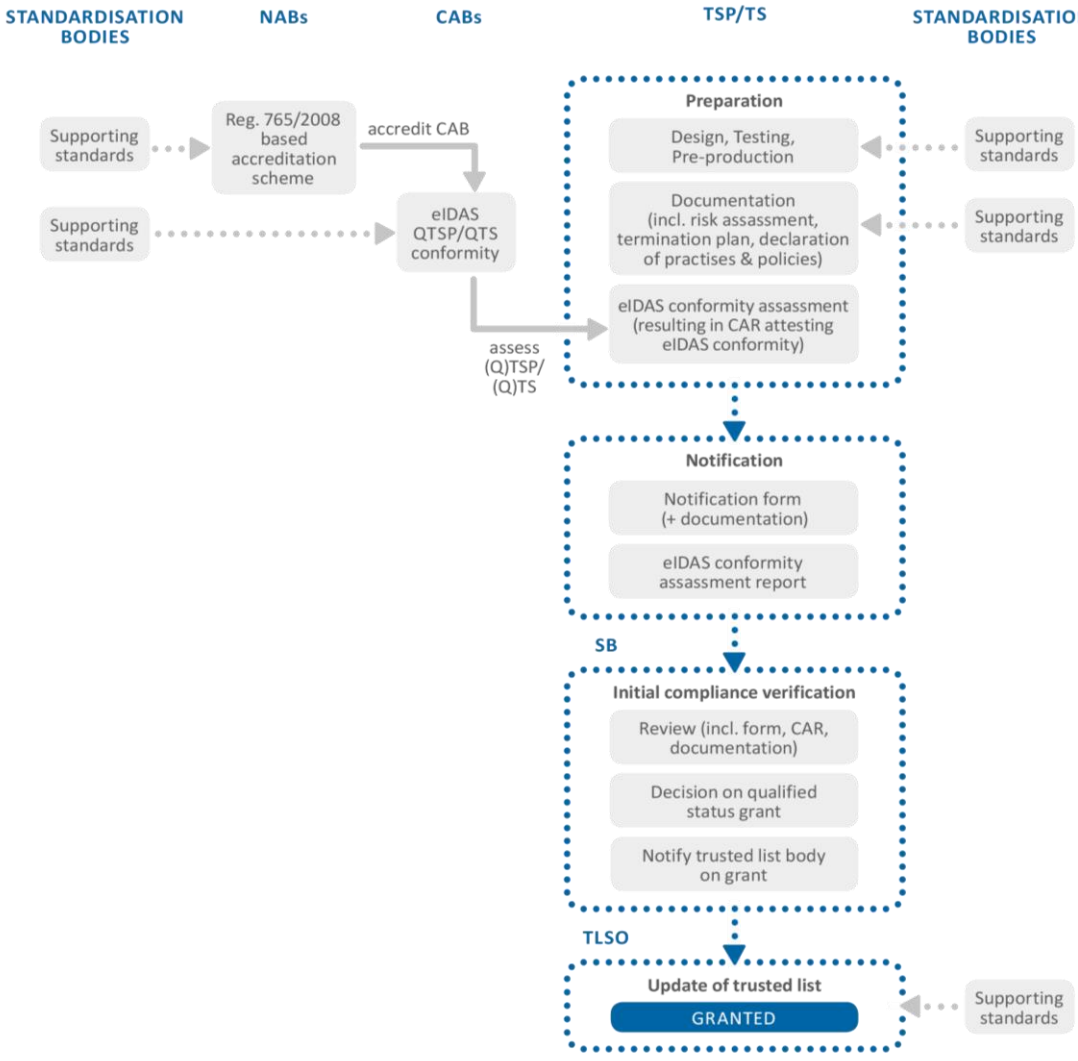

Figure 4 QTSP/QTS initiation process flow in the context of the eIDAS Regulation

4.4 eIDAS compliant accreditation schemes for CABs

4.4.1 eIDAS requirements for CAB accreditation schemes and for CAR

CABs

As identified in section 2.3, Art.3.18 of the eIDAS Regulation requires CABs to be accredited in accordance with Regulation (EC) No 765/2008 in a way that such accreditation ensures the accredited CABs are competent to carry out conformity assessment of a QTSP/QTS against the requirements of the eIDAS Regulation. Indeed, the conformity assessment is on QTSPs and QTSs which are eIDAS legal terms subject to requirements stemming from the eIDAS Regulation. They cannot be understood in a different context.

CARs

The resulting conformity assessment report to be submitted to the supervisory body by the assessed (Q)TSP, whether in the context of a 2-yearly regular audit (Art.20.1), an ad hoc audit (Art.20.2) or an initiation audit (Art.21.1) must be such that it confirms, when this is the case, that the assessed QTSP/QTS fulfil the requirements of all the applicable requirements of the eIDAS Regulation.

Provided the above requirements are met, it is a fact that it remains in the hands of MS to determine how the accreditation is done. In other words, MS remain free to set up any accreditation scheme provided that they can demonstrate that it fulfils Art.3.18 of the eIDAS Regulation.

Conformity assessment scheme

The conformity assessment scheme (including requirements on the CAB, requirements on the auditing rules under which the CAB will carry out their conformity assessment and the effective set of criteria, control objectives and controls against which it will assess a QTSP/QTS with the aim of confirming that it fulfils the eIDAS requirements) may be defined by the CAB itself, the EU MS supervisory body, or any other body possessing the necessary technical competence.[30]

NABs

The eIDAS Regulation requires, as part of the accreditation of the CAB, an evaluation by the competent NAB of that assessment scheme and of the competence of the CAB employing such an assessment scheme to carry out conformity assessment of a QTSP/QTS against eIDAS (Art.3.18). The competence of a CAB cannot be confirmed by any other entity than the competent NAB.

The accreditation of CABs, in accordance with Regulation (EC) No 765/2008, is the exclusive competence of NABs. CABs established in a EU MS are required to be accredited by the NAB of the EU MS in which they are established unless that NAB does not have the possibility to do so, in which case the CAB can request another NAB from another EU MS to conduct its accreditation.

Supervisory bodies

The “procedural” question regarding the eligibility of an eIDAS compliant CAR for its submission to a SB, and hence its admissibility by the SB under Art.21.1, Art.20.1 ,or Art.20.2 is not whether the report is fine to demonstrate that the assessed QTSP/QTS complies with the eIDAS requirements but whether it is formally a conformity assessment report issued by a conformity assessment body which is accredited in accordance with Regulation 765/2008 as competent to carry out conformity assessment of a qualified trust

[30] The entity defining and owning a conformity assessment scheme is denoted as the scheme owner.
A conformity assessment scheme will be called a certification scheme when the CAB is a certification body.

service provider and the qualified trust services it provides against the requirements of the eIDAS Regulation.

The format and content of a CAR should nevertheless be such that it contains sufficient information to demonstrate to the SB that each and every applicable requirement from the eIDAS Regulation for QTSPs and QTSs are indeed fulfilled by the assessed QTSP/QTS.

An eIDAS conformity assessment scheme must be defined in such a way that neither the business nor the technical model is imposed upon a QTSP/QTS nor a specific standard to be followed. A QTSP providing a QTS is free to define the way it implements the applicable eIDAS requirements, whether operationally, organisationally or technically. The (Q)TSP/(Q)TS has to demonstrate its compliance (building upon standards if it deems it appropriate) with the requirements of the eIDAS Regulation while the supervisory body cannot refuse to grant the qualified status solely on the grounds that the proposed model does not comply with a given standard or a given business/technical model. Consequently, in the absence of formal assessment of one or more technical standards and its/their referencing in an eIDAS implementing act for the presumption of compliance with the eIDAS requirements, a conformity assessment scheme cannot be compliant with the eIDAS requirements when the QTSP/QTS audit criteria against which the (Q)TSP/(Q)TS is assessed is limited to a (set of) standard(s). An eIDAS compliant conformity assessment scheme should hence be designed in such a way that those QTSP/QTS audit criteria are not defined in a “normative approach” (i.e. on the basis of a required compliance with a specific standard or on the basis of a specific technical way to proceed) but in an “outcome based approach” (i.e. ultimately the eIDAS requirements applicable to QTSP/QTS which are expressed in a technology-neutral way and expressing the goal to be reached). The definition of an “outcome based” conformity assessment scheme can build on standards or parts of them when assessed.

4.4.2 The EA promoted accreditation scheme for CABs assessing TSP/TS

The European cooperation for Accreditation (EA), is the body recognised under Regulation (EC) No 765/2008 that manages a peer evaluation system among NABs from the EU Member States and other European countries. That rigorous and transparent peer evaluation system ensures the equivalence of the accreditation services delivered by NABs and thus the equivalence of the level of competence of CABs. This mandatory peer evaluation system facilitates the mutual recognition and promotes the overall acceptance of accreditation certificates and conformity assessment results issued by accredited bodies. National authorities shall recognise the equivalence of the services delivered by those accreditation bodies (i.e. the NABs) which have successfully undergone such peer evaluation, and thereby accept the accreditation certificates of those bodies and the attestations issued by the CABs accredited by them.

The EA is also the recognised body, under Regulation (EC) No 765/2008, as competent to develop sectoral or specific accreditation schemes. This may be done on request of the Commission but in the context of the eIDAS Regulation this has not been the case.

Nevertheless, the EA has promoted[31] the ETSI EN 319 403[32] standard on requirements for CABs to carry out conformity assessment of TSPs as one route to demonstrate conformity with relevant requirements of the

[31] EA Resolution 2014 (34) 22 and EA document EAGA(14)31.

[32] 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. This document builds on ISO/IEC 17065 to specify additional requirements for CABs and additional auditing rules under which CABs will have to carry out their conformity assessments of QTSPs and their QTSs

eIDAS Regulation through assessment by accredited CABs. The EN 319 403 defined accreditation scheme is such that:

(i) It requires the accreditation of the CAB to be based on ISO/IEC 17065[33];
(ii) It supplements the general requirements provided in ISO/IEC 17065 to provide additional dedicated requirements for CABs performing certification of trust service Providers and the trust services they provide towards defined criteria against which they claim conformance.

It does not, however, specify those criteria nor the certification scheme and needs to be considered as an accreditation "framework" for the conformity assessment of TSP against audit criteria. Those criteria need to be defined in such a way that they should:

(a) take into account specificities of the type of trust service to be assessed;
(b) ensure that all aspects of the TSP activity are fully covered; and
(c) be based on standards, publicly available specifications and/or regulatory requirements.

Consequently, the EA promoted accreditation scheme (ISO/IEC 17065 completed by ETSI EN 319 403) cannot be implemented unless such effective criteria, the related control objectives and controls are clearly defined in a way that the NAB can evaluate the competency of the CAB to conduct an assessment of a QTSP/QTS against them in order to assess its conformity with the eIDAS requirements and so that the accreditation cannot be contested. Their definition will be the purpose of the conformity assessment scheme that may be defined by the CAB itself, the EU MS supervisory body, or any other body possessing the necessary technical competence.[34] Individually or collectively, e.g. under mutual assistance foreseen by Art.18 of the eIDAS Regulation, supervisory bodies could establish such conformity assessment schemes for assessing QTSP/QTS eIDAS conformity, leveraging on standards, in a way allowing establishing a presumption of compliance of the assessed QTSP/QTS with eIDAS and of the accreditation of CABs to be compliant with eIDAS as well.[35]

It should be noted that the EA promoted accreditation scheme (ISO/IEC 17065 completed by ETSI EN 319 403), still to be completed by an "eIDAS conformity assessment scheme" as explained, is not mandatory and might not be the only basis for such accreditations as discussed in the next section.

4.4.3 Other conformity assessment schemes (as alternative to the EA promoted scheme)

All NABs from EU Member States and from EEA countries are members of the EA. The EA is also the recognised body, under Regulation (EC) No 765/2008, as competent to develop sectoral or specific accreditation schemes. The EA and all its members have promoted unanimously the above described ETSI

[33] ISO/IEC 17065:2012: Conformity assessment -- Requirements for bodies certifying products, processes and services.
[34] To this extent, ISO/IEC 17065 requires in substance (in its section 7.2.1) that the criteria against which QTSP/QTS are evaluated shall be those contained in specified standards and other normative documents. ETSI EN 319 403 extends this to "standards, publicly available specifications and/or regulatory requirements" while taking into account specificities of the type of trust service to be assessed and ensuring that all aspects of the TSP activity are fully covered). ISO/IEC 17065 also suggests considering ISO/IEC 17007 for guidance for developing normative documents suitable for the purpose of establishing criteria documents. When explanations are required as to the application of these documents for a specific certification scheme, ISO/IEC 17065 (in its section 7.2.2) requires them to be formulated by relevant and impartial committees (or persons) possessing the necessary technical competence, and made available by the certification body upon request.
[35] See last § of section 3.4.4.

EN 319 403 accreditation scheme. Such promotions are not formally binding but makes it a commonly agreed consensus to use it.

NABs do not specify conformity assessment schemes. A conformity assessment scheme owner could put forward its scheme for purpose of accreditation of CAB in accordance with the eIDAS Regulation at a national level and the local NAB would ensure that the scheme meets the accreditation requirements.

However it is likely when such a scheme would deviate from the one promoted at the European level by the EA, it would need to be recognised being in accordance with the eIDAS requirements (i.e. Art.3.18 and Art.20.1) and as an appropriate alternative to the EA promoted one in order to ensure the equivalence of the level of competence of accredited CABs, to facilitate mutual recognition and to promote the overall acceptance of accreditation certificates and conformity assessment results issued by those accredited CABs.

To be considered as conformant with the eIDAS Regulation, a conformity assessment scheme:

- Must be such that the rules under which the CAB shall carry out QTSP/QTS assessment against those conformity assessment requirements and the competence of the CAB to carry out such assessments have been accredited by a competent NAB under Regulation (EU) 765/2008.
    - The ETSI framework scheme based on EN 319 403, complementing requirements in ISO/IEC 17065, and an accreditation under ISO 17065 is an option already promoted at the European level by the EA.
    - Alternatives could be based on other accreditation frameworks (e.g. ISO 17043, ISO 17021) covering inspection bodies or laboratories as CABs provided they are properly completed by requirements on CABs that ensure the evaluation of their competence in assessing QTSP/QTS against all the applicable eIDAS requirements.
- Must be such that the purpose of the assessment is to confirm that the assessed QTSP/QTS fulfil the eIDAS requirements applicable to the type of QTSP/QTS being assessed (conformity assessment requirements).
    - The conformity assessment requirements should be designed in accordance with recommendations made in section 4.4.4 of this document.
    - Note that to this extent, the EA promoted ETSI framework accreditation scheme based on EN 319 403 must additionally be completed by the identification of the evaluation criteria against which the QTSPs/QTSs are to be evaluated and to be judged (in this case, certified) to comply with the eIDAS requirements. Such a completion can be done by the CAB itself, the EU MS supervisory body or any other body possessing the necessary technical competence.
- Must be such that the CAR includes sufficient demonstration and a formal statement that the QTSP/QTS meet the requirement laid down in the eIDAS Regulation.
    - The CAR report should be structured against recommendations provided in section 4.5 of this document.

Any conformity assessment scheme competing, with regards to the CAB requirements, with the ETSI EN 319 403 accreditation scheme promoted at EU level by the EA, would be equivalently suitable to that EA promoted scheme provided it would be promoted for purpose of accreditation at a national level by the local NAB or at the EU level by the EA and provided that it has been demonstrated that the competing scheme meets the requirements of the eIDAS Regulation and of Regulation 765/2008.

The adoption, convergence, or migration of schemes for the accreditation of CABs in accordance with the eIDAS Regulation towards the ETSI EN 319 403 scheme with the accreditation based on ISO/IEC 17065, as promoted at the EA level, is encouraged by EA document EAGA(14)31.[36]

When a CAB has been correctly accredited in accordance with the eIDAS Regulation, no SB could reject the CAR produced by such a CAB for the sole reason that the CAB is not accredited by their national NAB. The NAB having accredited such a CAB can be the national body of the same EU MS for which the SB is competent or be from another MS[37].

4.4.4 eIDAS QTSP/QTS criteria as part of an eIDAS conformity assessment scheme

With regards to the further definition and clarification of the effective criteria, the effective related control objectives and controls to be used by an accredited CAB to evaluate QTSP/QTS compliance with the eIDAS Regulation and for which the competency of the CAB will be accredited by the NAB, it is important to note that:

- First, no standard or normative document has been referenced so far by any secondary legislation (implementing acts) that would have been adopted pursuant to the eIDAS Regulation and that, when met, would give a legal presumption of compliance of the QTSP or QTS against all or a specific subset of the applicable requirements.
- Second, any situation that would impose compliance on a QTSP/QTS with a specific standard or normative document is prohibited as it would be in contradiction with the eIDAS Regulation principles. The eIDAS Regulation is technologically-neutral and QTSPs/QTSs are free to define the way they implement those applicable requirements, whether operationally, organisationally or technically.
- Third, the resulting CAR and the final and unambiguous conformity statement are the necessary elements for the QTSP/QTS to be effectively granted a qualified status by the competent SB. It is ultimately the SB to which the CAR is notified by the assessed QTSP that will take the decision to grant or not the qualified status to the assessed QTSP/QTS. Hence the resulting CAR needs to contain sufficient information to demonstrate, in detail to the SB, that the assessed QTSP/QTS fulfil the requirements laid down in the eIDAS Regulation and consequently deserves to be granted a qualified status. It is not regarded as suitable that the SB, which has the obligation to verify the compliance of the QTSP/QTS with the Regulation, will take its decision on the sole basis of a yes/no conformity assessment document or CAR.
- Fourth, the granularity of the scope of the assessment on the targeted trust service is the one used in EU Member State trusted lists. That granularity should correspond, per type of QTSP/QTS, to the "service digital identity" concept as defined by CID (EU) 2015/1505 laying down technical

[36] The EA document EAGA (14)31 lays down the migration considerations for both CABs and National Accreditation Bodies (NABs) in order to transition of EA members existing arrangements for CAB accreditation (e.g. based on EN 45011, ISO/IEC 17021 for delivering certification against ISO 27001 – including fulfilling ISO 27006, ISO 20000) towards EN 319 403. Unfortunately, this document may be misleading in the sense that it refers to TSP applicable conformity assessment technical specifications and standards as part of this migration. The identification of those specifications and standards must not be understood as indicating a mandatory conformance to assess QTSP/QTS eIDAS requirements; they only indicate migration from former versions of standards to newer standards replacing them (whenever a conformity assessment against a specific standard is required e.g. in the context of CA/Browser Forum requirements).

[37] This may be the case when a CAB is established in a EU MS where the NAB has not implemented any eIDAS accreditation scheme and it has been accredited by a NAB from another EU MS or even a third country being an EA MLA signatory. This may also be the case when the notifying TSP has contracted a CAB from another country that the one in which it is established.

specifications and formats relating to trusted lists pursuant to Article 22.5 of the eIDAS Regulation. Indeed, once the SB decides to grant a qualified status to a QTSP/QTS, it shall inform the body responsible for establishing, maintaining and publishing the national trusted list for the purposes of updating it accordingly. It is only when that granted qualified status has been indicated in the trusted list that the assessed QTSP may begin to provide the assessed qualified trust service. Hence it is also important that the scope of the assessment corresponds to, and identifies clearly, the "service digital identity(ies)" identifying the trust service to be granted a qualified status, for each type of qualified trust service considered by the eIDAS Regulation as specified by CID (EU) 2015/1505.

In order to benefit from QTSP/QTS criteria, related control objectives and controls, which are efficient to demonstrate QTSP/QTS conformity with all the eIDAS requirements, it is recommended:

- They are organised per type of QTSP/QTS;
- They are organised per requirement of the eIDAS Regulation applicable to a specific type of QTSP/QTS;
- They include sufficient set of criteria to confirm that the assessed QTSP/QTS meets the applicable eIDAS Regulation requirements;
- They ensure that all aspects of the TSP activity are fully covered;
- They take into account the outcome based approach to the eIDAS requirements and not impose specific ways, and in particular no specific standard, for the assessed QTSP/QTS to implement the applicable eIDAS requirements;
- In general, and in particular when based on standards or publicly available specifications:
    - they are supported by demonstration that the criteria coming from those standards or publicly available specifications are suitable for confirming that the specific applicable eIDAS requirement(s) they support an evaluation against are met;
    - they allow deviation from strict compliance to standards where the requirements from standards exceed or contradict the eIDAS requirements.

The effective eIDAS QTSP/QTS criteria may be defined by the CAB itself, the EU MS supervisory body or any other body possessing the necessary technical competence. As a last resort, it may be up to the CAB to establish the effective eIDAS QTSP/QTS criteria, related control objectives and controls it will use for assessing QTSP/QTS against the eIDAS Regulation and to demonstrate to the NAB that they are sufficient to confirm that a QTSP/QTS is meeting the applicable requirements of the eIDAS Regulation and that they have the competency to conduct an assessment against those criteria.

NABs do not specify conformity assessment schemes. Those schemes can be put forward by the scheme owner for purpose of accreditation and the NAB would ensure that the scheme meets the accreditation requirements. Where this is purely a national scheme this is done by the local NAB. Where, like the ETSI EN 319 403 accreditation scheme, the conformity assessment scheme owner wants it recognised across Europe it is done through the EA process.

The competent supervisory body may also possess the necessary (technical) competences and be entitled to define an eIDAS conformity assessment scheme relying on appropriate accreditation requirements. An argument for SB to define such schemes or to establish requirements on them or to establish reference number on specific standards with or without any adaptations of their requirements, is that the SB is the final entity to verify the conformity of QTSP/QTS with the eIDAS requirements and granting or withdrawing a qualified status. Supervisory bodies, when defining such criteria must pay attention to using an outcome based approach that does not require any specific (e.g. technical, operational, organisational) way to proceed and in particular does not require compliance with any specific technical requirement or technical

standard. A supervisory body may establish an eIDAS conformity assessment scheme on the basis of referenced technical specifications or standards, with or without amendments after assessment of their compliance with the requirements set in the Regulation, so that once the criteria are met by the corresponding QTSP/QTS they may benefit from a presumption of compliance with the applicable eIDAS requirements with regards to the supervisory body decision under Art.21.2 of the eIDAS Regulation.[38]

4.4.5 Consequence of the grant of a qualified status by a SB on the basis of a CAB and/or a CAR not conform the eIDAS Regulation

Considering that the CAR is only a tool facilitating a SB's task when deciding whether a notifying TSP (and the QTS it intends to provide) meet the requirements of the eIDAS Regulation and it does not bind the latter with regards to that decision, it could be considered that providing a CAR resulting from a conform audit carried out by a conform CAB (Art.3.18) is not a compulsory formality under penalty of nullity (provided that the information included in the CAR did not lead the SB to take a decision that is not conform to the eIDAS Regulation). This does not remove the obligation for CARs to meet the requirements of the eIDAS Regulation.

Withdrawing of a qualified status by a SB, for the sole reason that the SB has granted a qualified status on the basis of a CAR that was not eIDAS conformant would, nevertheless, not be appropriate (in particular when the QTSP/QTS does meet the eIDAS requirements) and this would not be considered as good administration since the competent authority considered, rightly or not, that the requirements regarding the procedural rules was met creating legitimate expectations from the QTSP and its users. However, in that case, the SB should be recommended to require an ad hoc audit to be carried out, within a reasonable short time frame, by a CAB accredited in accordance with the eIDAS Regulation and in compliance with the eIDAS requirements this time, in order to confirm the qualified status, i.e. that the concerned QTSP/QTS meet the eIDAS requirements.

4.5 Structure and content of the CAR

The conformity assessment report (CAR) referred to in Art.21.1 of the eIDAS Regulation is a prerequisite for the QTSP/QTS to be effectively granted a qualified status by the competent supervisory body (SB).

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

It is in the interest of the TSP to ensure that the CAR it receives from the accredited CAB that conducted its assessment brings indeed sufficient information that demonstrate that the TSP/TS complies with the requirements laid down in the eIDAS Regulation, and in particular, with the requirements for QTSP/QTS.

It would also be in the interest of the SB to edit some recommendations on the structure and content of the CAR referred to by Art.21.1 of the eIDAS Regulation so that it will be easier for the SB, in the

[38] See for example, the referenced specification documents applicable to the qualification of trust service providers and the trust services they provide (those documents are available in French only from the following website: http://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/documents-publies-par-lanssi/). For each type of QTSP/QTS, one or several documents provide, explicitly or by reference, a list of requirements that the French supervisory body consider, once met by QTSP/QTS, as meeting the referenced applicable eIDAS requirements.

boundaries of the principles of good administration and other similar applicable rules, to verify whether those requirements are met or not, and to argue that the received CAR does not meet the eIDAS requirements and/or does not bear sufficient information demonstrating the QTSP/QTS requirements are met.

The specifications with regards to the structure and content of the CAR referred to in Art.21.1 of the eIDAS Regulation are **recommended** to include at least the following[39]:

- [eIDAS – Art.20.1] Bear a clear conformity statement confirming - if such is the case - that the assessed QTSP/QTS meets all the applicable requirements of the eIDAS Regulation.
- [Recommendation] Provide sufficient details to demonstrate that the assessed TSP/TS fulfils the requirements laid down in the eIDAS Regulation, and in particular, the requirements for QTSP/QTS.

  Note: Those details and information demonstrating QTSP/QTS compliance with the eIDAS Regulation requirements may be included by reference to other reports, e.g. such as audit reports against technical standards, which contain detailed and herewith sufficient information for the SB to judge the QTSP/QTS conformity. On top of that the SB may need to refer to the security documentation of the TSP, like the security concept, its declaration of practices and/or of policies, etc., as it may be referenced in the CAR.

- [Recommendations] In order to bear sufficient details to demonstrate such a fulfilment the structure and the information provided should:

  1) Clearly identify the name of the CAB, and where applicable its registration number, as stated in the official records, its official postal address and its electronic address.
  2) Clearly identify the name of the national accreditation body (NAB) having accredited the CAB, and where applicable the registration number, as stated in the official records, the official postal address and electronic address of the NAB.
  3) Include the accreditation certificate or a link to the location from where the accreditation certificate issued by the NAB identified in accordance with point (2) together with the detailed description or a link to the location from where the detailed description of the underlying accreditation scheme including indication of its relevance to the eIDAS Regulation can be retrieved.

     Note: The CAB accreditation certificate, the CAR should clearly identify the accreditation scheme under which the CAB has been accredited in the context of Reg.765/2008 (e.g. ISO/IEC 17065 being completed by ETSI EN 319 403) and the conformity assessment scheme for which the CAB has been accredited to conduct conformity assessment of TSP/TS against the requirements laid down in the eIDAS Regulation, and in particular, against the requirements for QTSP/QTS.

  4) Include the accredited conformity assessment scheme document (i.e. QTSP/QTS audit criteria) or a link to the location from where that document is available.
  5) Clearly identify the name of the CAB lead auditor having issued [and signed] the CAR.
  6) Clearly identify the name of the assessed trust service provider, and where applicable its registration number, as stated in the official records, its official postal address and its electronic address.
  7) Clearly identify the conformity assessment target trust service(s) of the TSP for which the CAR confirms the conformity with the requirements of the eIDAS Regulation. The identification of the

[39] Each bullet is preceded by an indication whether the item is a requirement from the eIDAS Regulation or a recommendation of the present guidance document.

service(s) is to align with CID (EU) 2015/1505 and clause 5.5.1.1 of ETSI TS 119 612 v2.1.1 (note: to this extent this should include at least the RFC 5280 Subject Key Identifier or the public key of the target trust services and the Base64 PEM representation of the associated X.509 v3 digital certificate; additionally it should also distinguish, when applicable, whether specific sets or sub-sets of certificates should be excluded from the confirmation of conformity and on which criteria they can be identified).

8) Provide for each qualified trust service identified in point (7)[40] a detailed description of the (e.g. PKI) functional architecture or hierarchy with the purpose to allow identification of the service(s) to be listed in the applicable national trusted list in accordance with CID (EU) 2015/1505.

   Such detailed description may be included by reference to other reports. When this is the case, a precise and non-ambiguous summary of the TSP and the services covered should appear in the CAR.

   That description should also clearly identify which QTS components or service components are operated by third parties (e.g. subcontractors) and their locations.

   Note: A QTSP can make use of third parties, whether (Q)TSPs or not, to operate part or all of the components or component services of the (Q)TS they provide. In this situation, the QTSP remains the final entity responsible and liable for the QTS he provides and needs to document and ensure correct implementation of those component services against his declared practices and policies and of course against the eIDAS requirements.

9) Identify an exhaustive list of public and TSP internal documents that have been part of the scope of the audit. The public documents should either be attached to the CAR or publicly accessible links should be provided allowing for a download of those documents.
   Public documents should include, as a minimum:
   a) The declaration of the practices used by the TSP to provide the qualified trust services;
   b) The qualified trust service policy(ies), i.e. the set of rules that indicates the applicability of the qualified trust service to a particular community and/or class of application with common security requirements.
   c) Subscriber agreement and related terms and conditions.

   Internal documents should include, as a minimum:
   a) The termination plan referred to in Art.24.2.(i) of the eIDAS Regulation.
   b) The documentation related to the assessment of risks aimed at supporting the demonstration of the requirements of eIDAS Regulation Art.19.1.
   c) A security & personal data breach notification plan aimed to support demonstration of the requirement of eIDAS Regulation Art.19.2.
   d) The list of all internal documents supporting the declaration of the practices used by the TSP to provide the qualified trust services and the qualified trust service policy(ies).

10) Identify, for each stage of the audit (e.g. documentation audit and implementation audit including onsite inspections), the period during which the audit has been conducted (elapsed time) and the effort in man-days engaged by the CAB to conduct the audit.
11) Provide, for each of the following eIDAS requirements, a report on the fulfilment by the TSP and by the implementation of its qualified trust services of the identified requirement, or when appropriate, on the existence of proper procedures and management system for handling this

[40] See also Annex A.7.

requirement. Those reports should identify the detailed audit controls and control objectives that have been conducted during the audit to establish them with an indication of each non-conformity and their level of importance (or a reference to separately available audit reports in which such information is included; such audit reports shall be attached to the CAR):

a) General requirements for qualified TSPs and for each type of qualified trust services (with an indication of the relevant articles of the eIDAS Regulation)
   i) Data processing and protection (Art.5)
      (1) Art.5.1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.
   ii) Provisions on liabilities meet the Art.13 requirements:
      (1) (Art.13.1) The TSP liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation
         (a) Burden of proving intention/negligence of a non-qualified TSP lies on the claiming party.
         (b) Intention or negligence of a QTSP shall be presumed, unless proven otherwise by QTSP.
      (2) (Art.13.2) When the TSP informed customer in advance on limitations on the use of their services, & when such limitations are recognisable to third parties, the TSP is not liable when the limitations have been exceeded.
      (3) (Art.13.3) In accordance with national rules on liability.
   iii) Accessibility for person with disabilities (Art.15)
   iv) Due diligence (Art.19.1)
      (1) The TSP shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide.
      (2) Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk.
      (3) Measures shall be taken to prevent and minimize the impact of security incidents and inform stakeholders of the adverse effects of any such incidents
   v) Security & personal data breach notification (Art.19.2)
      (1) The TSP shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.
      (2) The TSP shall also notify the [likely adversely affected] natural or legal [customer] of the breach of security or loss of integrity without undue delay.
      (3) May be required by the supervisory body to inform the public, when it is in the public interest.
   vi) Art.20 Supervision of qualified trust service providers
      (1) The TSP ensures that it is audited at least every 24 months by an accredited CAB in order to confirm fulfilment of the requirements of the eIDAS Regulation.
      (2) The TSP allows the competent supervisory body and a CAB to audit the compliance with the requirements of the eIDAS Regulation.
      (3) Where the supervisory body requires from the TSP to remedy any failure to fulfil requirements under the eIDAS Regulation, the TSP will act accordingly within the set deadline.

vii) Art.23 on the correct use, when applicable, of the EU trust mark for qualified trust services (including provisions from CIR (EU) 2015/806.
viii) Art.24.2 of the eIDAS Regulation:
(a) Inform SB of any change in QTS provisioning and of intention to cease;
(b) Requirements on staff;
(c) Sufficient financial resources and/or liability insurance, in accordance with national law;
(d) Consumer information on terms and conditions, incl. limitations on use;
(e) Use trustworthy systems and products;
(f) Use trustworthy systems to store (personal) data;
(g) Take appropriate measures against forgery and theft of data;
(h) Record and keep accessible data related to activities, issued and received, even after cessation;
(i) Up-to-date termination plan (to be agreed with SB) to ensure continuity of service;
(j) Ensure lawful processing of personal data in accordance with Directive 95/46/EC.

b) Additional specific requirements for the applicable type of qualified trust service
i) Qualified certificate for electronic signatures
(1) Art.24.1.(a) to (d)
(2) Art.24.2.(k)
(3) Art.24.3
(4) Art.24.4
(5) Art.28.1 – Annex I
(6) Art.28.2
(7) Art.28.3
(8) Art.28.4
(9) Art.28.5
ii) Qualified certificate for electronic seals
(1) Art.24.1.(a) to (d)
(2) Art.24.2.(k)
(3) Art.24.3
(4) Art.24.4
(5) Art.38.1 – Annex III
(6) Art.38.2
(7) Art.38.3
(8) Art.38.4
(9) Art.38.5
iii) Qualified certificate for website authentication
(1) Art.24.1.(a) to (d)
(2) Art.24.2.(k)
(3) Art.24.3
(4) Art.24.4
(5) Art.45.1 – Annex IV
iv) Qualified validation service for qualified electronic signatures (Art.33.1)
v) Qualified validation service for qualified electronic seals (Art.40)
vi) Qualified preservation service for qualified electronic signatures (Art.34.1)
vii) Qualified preservation service for qualified electronic seals (Art.40)
viii) Qualified electronic time stamps (Art.42.1.(a) to (c))
ix) Qualified electronic registered delivery services (Art.44.1.(a) to (f))

12) Provide, when the conformity is additionally confirmed or certified as compliant against a specific standard or publicly available specifications, the report on the fulfilment by the TSP and by the implementation of its qualified trust services against such standard or specifications that has been conducted during the audit, as separate documents with an indication of the non-conformities and their level of importance.
13) Detail the list of the third parties entrusted by the TSP to perform all or parts of its processes supporting the provision of its qualified trust services. The CAR should detail which of these parties have been subject to the audit.
    Note: If already provided otherwise, e.g. in an additional audit report as specified under point (12), this should not be required to be repeated.
14) Indicate, when required by the applicable accreditation/conformity assessment scheme, by when the next surveillance audit and the next compliance audit have to be conducted at the latest.[41]
15) Indicate under which circumstances an accredited conformity assessment body has to be involved in reassessing the assessed TSP and the qualified trust services in addition to the planned audits.

The CAR should be clearly requested to be protected in integrity (since it is sent by the QTSP and not directly by the CAB) and to ensure its origin. To this extent, the CAR should be requested to be either signed using the handwritten signature of the CAB lead auditor, signed using an advanced electronic signature, sealed with an advanced electronic seal of the CAB, or by some equivalent method.
The confidentiality of the information notified by the (Q)TSP (incl. the CAR) to the SB should be ensured (since it may contain sensitive information).

4.6 Notification of accredited CABs and conformity assessment activities

The eIDAS Regulation does not foresee any obligation for the EU MS or the NABs to notify or inform of the conformity assessment activities in respect of which accreditation of CAB is operated in accordance with this Regulation and of any changes thereto, in particular information on the accredited CABs and the accreditation scheme details.

Regulation (EC) No 765/2008 only foresees an obligation for a NAB to inform the other NABs of the conformity assessment activities in respect of which it operates accreditation and of any changes thereto, and not to inform any other body or the Commission of those activities (Art.12.1). That Regulation also limits the obligation of each EU MS to inform the Commission and the EA on the communication of the identity of its NAB and of all conformity assessment activities only in respect of which that body operates accreditation in support of Community harmonisation legislation (Art.12.2). This includes details about the CABs accredited to carry out third-party conformity assessment tasks, on conformity assessment activities/modules, products concerned, and attestation of competence. All the notified CABs and the associated notifications are expected to appear in the NANDO database (http://ec.europa.eu/growth/tools-databases/nando/).

The use of the NANDO database is governed by the EC as it is specifically designed for new approach directives and notified bodies. Hence, it may not be expected that NANDO will include a specific repository of eIDAS accredited CABs notified to the Commission by the MS as NANDO is a very specific database that lists notified bodies. Notified bodies are bodies that have been appointed by Member States to the Commission and other Member States to carry out conformity assessment activities in the field of so called

[41] The annual surveillance audit that may be a requirement coming from the accreditation/conformity assessment scheme under which CAB are accredited and (Q)TSP/(Q)TS are audited (e.g. §7.9 of ISO 17065 and EN 319 403) is not a requirement from the eIDAS Regulation.

New Approach and New Legislative Approach Legislation. Only notified bodies are allowed to carry out these tasks.

It should be clarified (e.g. by the EC) whether either an obligation or a possibility or on the contrary any prevention would exist for MS to notify the EC for publication in the NANDO database of the CABs accredited in accordance with the eIDAS Regulation.

As a general recommendation, notified information should also include information, and any change thereto, about each of the EA MLA signatory NABs, whether they operate an accreditation scheme in accordance with the eIDAS Regulation, details regarding such an accreditation scheme, accredited CABs and for which QTPS/QTS, accredited CABs conformity assessment activities (e.g. certification certificates), etc. The database eventually used for the publication of such information, the practical aspects (e.g. identification of the notification bodies; location, content and structure of page related to eIDAS accreditation of CABs) should be organised in such a way that the information could easily be consumed by relying parties including TSPs and SBs.

On the other hand, in general, conformity assessment certificates, if provided by accredited CABs, need to carry the logo of the accreditation body that has accredited them. In this respect, it may be possible to find out whether a certificate has been issued by an accredited CAB or not, by which NAB it has been accredited and under which accreditation scheme. However, this requires a careful analysis of such conformity assessment certificates. That may be quite straightforward for SB receiving the initially notified or 2-yearly CAR but it does not solve the need of TSPs or QTSPs to benefit from market information and identify which are the candidate CABs being duly accredited to conduct assessment activities in accordance with the eIDAS Regulation.

It is recommended to NABs, and alternatively to SBs under Art.18 of the eIDAS Regulation, to cooperate to set-up a single and centralised dissemination point providing to the public, information, and any change thereto, about each of the EA MLA signatory NABs, whether they operate an accreditation scheme in accordance with the eIDAS Regulation, details regarding such an eIDAS accreditation scheme, eIDAS accredited CABs and for which type(s) of QTPS/QTS, eIDAS conformity assessment activities (incl. certificates when available) carried out by eIDAS accredited CABs, etc.

As an illustrative example for a very limited number of EU MS, that information could be made available as detailed and displayed in the following figures[42].

[42] Examples data based on information available by 21.09.2016.

EU MS PROFILE: BELGIUM

NATIONAL ACCREDITATION BODY

Name: **BELAC**
Website: www.belac.fgot.be
Email: belac@econimie.fgot.be

EIDAS SUPERVISORY BODY

Name: **Be.Sign (SPF Economy)**
Website: www. econimie.fgot.be
Email: be.sign@econimie.fgot.be

EIDAS ACCREDITATION SCHEME

Adoption of EA scheme: YES
a) Gen. framework: Regulation (EC) 765/2008 against ISO 17065
b) Specific scheme: ETSI EN 319 403 v2.2.2.
c) eIDAS Reg. 910/2014/EU applicable requirements for each QTP/QTS type
Instantiation of c) wrt. QTSP/QTS audit criteria: YES
→ Defined by CAB: YES; Defined by NAB: n.a. ; Defined by SB: n.a.
Location of detailed description: ???
Alternative equivalent scheme: NO
If YES, equivalence judged by: n.a.
Specific rules for CAR content and structure: ???

LIST OF ACCREDITED CABS

Accredited CABs	Accreditation certificate (URI)
–	–

LIST OF ASSESSED QTSPS/QTSS

QTSP	QTS	aCAB	Certificate of conformity (URI)
–	–	–	–
–	–	–	–

Figure 5 Example (BE) of EU MS illustrative profile regarding accreditation of CABs in accordance with the eIDAS Regulation

EU MS PROFILE: ESTONIA

NATIONAL ACCREDITATION BODY

Name: **EAK**
Website: www.eak.ee
Email: info@eak.ee

EIDAS SUPERVISORY BODY

Name: **Tehnilise Jarelevalve Amet**
Website: http://sr.riik.ee/en.html
Email: info@tja.ee

EIDAS ACCREDITATION SCHEME

Adoption of EA scheme: NAB not ready
a) Gen. framework: Regulation (EC) 765/2008 against ISO 17065
b) Specific scheme: ETSI EN 319 403 v2.2.2.
c) eIDAS Reg. 910/2014/EU applicable requirements for each QTP/QTS type
Instantiation of c) wrt. QTSP/QTS audit criteria: NAB not ready
→ Defined by CAB: n.a. ; Defined by NAB: n.a. ; Defined by SB: n.a.
Location of detailed description: NAB not ready
Alternative equivalent scheme: NO
If YES, equivalence judged by: n.a.
Specific rules for CAR content and structure: NAB not ready

LIST OF ACCREDITED CABS

Accredited CABs	Accreditation certificate (URI)
–	–

LIST OF ASSESSED QTSPS/QTSS

QTSP	QTS	aCAB	Certificate of conformity (URI)
SK	CA/QC for eSeals	TÜVIT (DE)	http://sr.riik.ee/sites/default/files/9704UE_s.pdf
SK	TSA/QTST	TÜVIT (DE)	http://sr.riik.ee/sites/default/files/9703UE_s.pdf

Figure 6 Example (EE) of EU MS illustrative profile regarding accreditation of CABs in accordance with the eIDAS Regulation

EU MS PROFILE: GERMANY

NATIONAL ACCREDITATION BODY

Name: **daKKs**
Website: www.dakks.de
Email: contact@dakks.de

EIDAS SUPERVISORY BODIES

Name: **Bundesnetzagentur**
Website: www.bundesnetzagentur.de
Email: eIDAS@bnetza.de
Name: **BSI**
Website: www.bsi.bund.de
Email: bsi@bsi.bund.de

EIDAS ACCREDITATION SCHEME

Adoption of EA scheme: YES
a) Gen. framework: Regulation (EC) 765/2008 against ISO 17065
b) Specific scheme: ETSI EN 319 403 v2.2.2.
c) eIDAS Reg. 910/2014/EU applicable requirements for each QTP/QTS type

Instantiation of c) wrt. QTSP/QTS audit criteria:
→ Defined by CAB: yes ; Defined by NAB: no. ; Defined by SB: no

Location of detailed description:
http://www.dakks.de/content/antrag-zur-pr%C3%BCfung-der-akkreditierungsf%C3%A4higkeit-von-konformit%C3%A4tsbewertungsprogrammen
http://www.dakks.de/content/kombinierte-chcklistebericht-bewertung-von.neuen-konformit%C3%A4tsbewertungsprogramen-nach-71

Alternative equivalent scheme: no

Specific rules for CAR content and structure: (see above description)

LIST OF ACCREDITED CABS

Accredited CABs	Accreditation certificate (URI)
T-systems International GmbH	http://www.t-systems-zert.de/pdf/akkred_urkunden/DAkkS_Urkunde.PDF
TUV Informartionstechnik GmbH	http://www.dakks.de/as/ast/d/D-ZE-12022-01-01.pdf
Datenschutz cert GmbH	https://www.datenschutz-cert.de/fileadmin/datenschutz-cert/media/Downloads/SigG-eIDAS/Urkunden/dsc_DAkkS_Konformitaetsbewertungsstelle_eIDAS_2016.pdf

LIST OF ASSESSED QTSPS/QTSS

QTSP	QTS	aCAB	Certificate of conformity (URI)
Bundesagentur fuer Arbeit	TSA/QTST	T-Systems International GmbH	???
Bundesnotarkammer	TSA/QTST	TÜV Informationstechnik GmbH	https://www.tuvit.de/data/content_data/tuevit_de/9710UD_s.pdf
D-TRUST GmbH	TSA/QTST	TÜV Informationstechnik GmbH	https://www.tuvit.de/data/content_data/tuevit_de/9707UD_s.pdf
DGN Deutsches Gesundheitsnetz Service GmbH	TSA/QTST	T-Systems International GmbH	https://www.t-systems-zert.de/pdf/ein_03_sig_zda/zf_031.0252_d.pdf
Exceet Secure Solutions AG	TSA/QTST	TÜV Informationstechnik GmbH	https://www.tuvit.de/data/content_data/tuevit_de/9702UD_s.pdf
Deutsche Rentenversicherung Bund	TSA/QTST	TÜV Informationstechnik GmbH	https://www.tuvit.de/data/content_data/tuevit_de/9709UD_s.pdf
1&1 De-Mail GmbH	EDS/REM/Q	TÜV Informationstechnik GmbH	https://www.tuvit.de/data/content_data/tuevit_de/9711UD_s.pdf
Mentana-Claimsoft GmbH	EDS/REM/Q	TÜV Informationstechnik GmbH	https://www.tuvit.de/data/content_data/tuevit_de/9713UD_s.pdf

Figure 7 Example (DE) of EU MS illustrative profile regarding accreditation of CABs in accordance with the eIDAS Regulation

5. Format and procedure of notification under Art.21.1 of the eIDAS

The procedure for notification under Art.21.1 of the eIDAS Regulation should be clearly established and communicated to TSPs.

It is **recommended** that:

(a) Such a procedure is made publicly available from the website of the national supervisory body (SB).
(b) The notification is supported by a notification form to be completed by the notifying TSP and sent to the competent SB.
(c) The completed notification form should be either signed using the handwritten signature of a legal representative of the notifying TSP, or signed using a qualified electronic signature or sealed with an qualified electronic seal.
(d) Where required by national law, the notifying TSP includes proof that the person signing the notification form is legally representing the TSP organisation. For example, by including an extract from official records like a national trade register.
(e) The confidentiality of the information notified by the TSP to the SB should be ensured (as it may contain sensitive information).
(f) The signature/seal on the notification form should be compliant with the applicable signature format standard referred to in Commission Implementing Decision (EU) 2015/1506[43].
(g) The notification form indicates the documentation to be submitted jointly with the notification form as part of the notification (see below for recommendation on that documentation).
(h) The completed, signed or sealed, notification form and related documentation are sent electronically to the competent SB, or as an alternative, delivered by hand or postal mail.
(i) The notification form clearly indicates or refers to the relevant fees, when applicable, that the TSP will have to pay for the competent SB services, from the notification until the termination of the notified trust services and/or the withdrawal of the qualified status would it be granted by the SB, and whether those fees are fixed or recurrent fees or a mix of both.
(j) The competent supervisory body acknowledges receipt of the notification within time limit defined in national law of each MS (e.g. within three working days of its receipt), providing clear indication to the notifying TSP:
    (i) Acknowledgement of receipt should not in any manner be interpreted as signifying that the SB considers that the TSP complies with the requirements of the eIDAS Regulation and any other relevant requirements under national legislation;
    (ii) The obligations or a reference to the obligations of the competent SB, including, when applicable, reference to applicable legislation;
    (iii) The obligations or a reference to the obligations of the notifying TSP, including, when applicable, reference to applicable legislation;
    (iv) The next steps of the process leading to the grant of a qualified status, when applicable, to the notified TSP and the notified trust service(s) it intends to provide.

[43] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 235, 9.9.2015, p. 37–41.

(k) The notification procedure documentation and/or the notification form should include a reference to the security breach and personal data breach incident report procedure and form allowing TSPs to notify the supervisory body in accordance with Art.19.2 of the eIDAS Regulation.

The documentation to be submitted jointly with the notification form as part of the notification under Art.21.1 of the eIDAS Regulation is **recommended** to include at least the following:

1) A conformity assessment report (CAR) issued by a conformity assessment body (CAB) duly accredited as per the requirements of the eIDAS Regulation.

   Note: The notification form should clearly indicate the expectations, recommendations or requirement with regards to the required CAR and the issuing CAB, e.g. that:

   a) The competent SB recognises a CAB as duly accredited as per the requirements of the eIDAS Regulation when the CAB has been accredited by a national accreditation body under Regulation (EC) No 765/2008 and when the accreditation certificate certifies that the CAB:
      i) Fulfils the requirements of the standard ISO/IEC 17065:2012, and
      ii) Fulfils the requirements of the standard ETSI EN 319 403 V2.2.2 (2015-08), and
      iii) Has the skills and competencies to certify that TSP/TS comply with the requirements laid down in the eIDAS Regulation, and in particular, with the requirements for QTSP/QTS, on the basis of a conformity assessment scheme for which the CAB is accredited.
   b) The competent SB recognises a CAB as duly accredited as per the requirements of the eIDAS Regulation when the CAB has been accredited by a national accreditation body under Regulation (EC) No 765/2008 under another normative scheme as the one specified in 1.(a) provided such an alternative scheme has been recognised as conform to the eIDAS requirements (Art.3.18, Art.20.1).
   c) The purpose of the CAR is to assess the conformity of TSP/TS with the requirements laid down in the eIDAS Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services concerned by the notification. Consequently, the CAR must bear a clear conformity statement confirming - if such is the case - that the assessed QTSP/QTS meets all the applicable requirements of the eIDAS Regulation.
   d) The CAR is to provide sufficient details to demonstrate that the assessed QTSP/QTS meets all the applicable requirements of the eIDAS Regulation.
   e) The structure and the information provided in the CAR should be aligned with the specifications provided in the notification form (see section 4.5 of this document for guidance on the recommended structure of such a report).

2) Memorandum and Articles of Association of the notifying TSP.
3) Evidence that the notifying TSP maintains sufficient financial resources and/or has obtained appropriate liability insurance with regards to the provision of the trust services for which a qualified status is requested, e.g. including

   a) Copy of the profit and loss account and balance sheets for the last 3 years for which accounts have been closed; failing that, appropriate statements from banks[44].

[44] Subject to applicable national laws, if, for some exceptional reason (to be notified with its justification by the notifying TSP) which the competent SB considers justified, the notifying TSP is unable to provide one or other of those documents, it may prove having sufficient financial resources by any other document which the competent SB

b) Liability insurance statements.

4) Trust service policy(ies) that applies(apply) to the trust services for which a qualified status is requested.
5) Trust service practice statement that applies(apply) to the trust services for which a qualified status is requested.
6) Trust service detailed architecture (e.g. PKI hierarchy along with the indication of the supported trust service policies) of the trust services for which a qualified status is requested.
7) Test samples of all relevant and applicable types of outputs from the qualified trust services the notifying TSP intends to start providing.
8) List of standards:
   a) with which operations are claimed to be compliant.
   b) with which operations are audited, evaluated, certified or assessed to be compliant and details about the underlying audit, evaluation, certification or assessment scheme.
9) Copy of standard end-user agreement the notifying TSP intends to use with regards to the provision of the trust services for which a qualified status is requested.
10) The documentation related to the assessment of risks aimed at supporting the demonstration of the requirements of eIDAS Regulation Art.19.1.
11) A security & personal data breach notification plan aimed to support the demonstration of the requirements of eIDAS Regulation Art.19.2.
12) The termination plan (eIDAS Regulation Art.17.4.(i), Art.24.2.(i)).

In addition to any applicable national language, all relevant documents regarding format and procedure for notification under Art.21.1 of the eIDAS Regulation should be made available in UK English in order to facilitate eIDAS Art.18 cooperation between EU MS SBs, when applicable.

The confidentiality of the information notified by the (Q)TSP to the SB should be ensured (since it may contain sensitive information).

considers appropriate. The competent SB may reserve the right to request any other document enabling it to verify the TSP's financial resources.

6. Initial verification of the notified QTSP/QTS with the eIDAS requirements & communication of the granted qualified status for inclusion in the national TL

As previously stated in the present document, it is ultimately the supervisory body (SB) that will take the decision to grant or not the qualified status to the notifying QTSP/QTS.

In order to enable and facilitate the task of the SB in taking a proper and informed decision, it is crucial that the notification submitted by the notifying TSP and in particular that the submitted CAR includes sufficient information to demonstrate, in detail to the SB, that the assessed QTSP/QTS fulfil the requirements laid down in the eIDAS Regulation and consequently deserves to be granted a qualified status. It is not regarded as suitable that the SB, which has the obligation and bears the final liability to verify the compliance of the QTSP/QTS with the eIDAS Regulation, will take a positive decision on a Conformity Assessment Report, when the underlying conformity assessment (e.g. certification) has been done against a specific standard and not against the eIDAS requirements.

In order to allow for an efficient initiation process, as stressed by Recital (45) of the eIDAS Regulation, preliminary interactions between prospective qualified trust service providers and the competent supervisory body are encouraged with a view to facilitating the due diligence leading to the provisioning of qualified trust services.

The following assumptions can be regarded concerning the “initial verification” phase:

- The SB has communicated to candidate TSPs the applicable national requirements and recommendations regarding the notification procedure, the notification form, the accompanying documentation and the CAR, as recommended in the present document, and
- The notifying TSP has implemented those requirements and recommendations.

However, the following recommendations on the steps to be undertaken by the notified SB, can be applied even the above assumptions are not met:

1) On reception of a notification under Art.21.1 from a TSP intending to start providing qualified trust services, acknowledge the reception to the TSP (see section 4.(k)).
2) Verify that the notification procedure has been respected, e.g. that the notification form is fully completed, duly signed, accompanied with the required documentation (see section 4 for guidance on recommendations for such a documentation) and in particular verify the eligibility of the CAR. Verification of the eligibility of the CAR includes verification that
   (a) The CAR has been issued by a CAB accredited in accordance with the eIDAS Regulation (see section 0).
   (b) The CAR provides sufficient information to demonstrate that the assessed QTSP/QTS fulfil each of the applicable eIDAS requirements (see section 4.5).

   When this verification is not satisfactory, indicate the non-conformities to the notifying TSP as well as the deadline for correcting these non-conformities.
3) Clearly identify the name of the assessed trust service provider, and where applicable its registration number, as stated in the official records, its official postal address and its electronic address.

Note: Both the notification form and the CAR should bear that information. The related information from the notification form and the CAR should of course match.

4) Clearly identify the qualified trust service(s) of the trust service provider for which the CAR confirms (e.g. certifies) the conformity with the requirements of the eIDAS Regulation. The identification of the service(s) is to align with CID (EU) 2015/1505 and clause 5.5.1.1 of ETSI TS 119 612 v2.1.1.

   Note: Both the notification form and the CAR should bear that information. The related information from the notification form and the CAR should of course match. At least the CAR should provide that information to the level of details required to allow identification of the service(s) to be listed in the applicable national trusted list in accordance with CID (EU) 2015/1505 (see section 2.4 of the present document).

5) Taking into account, for each (potentially) qualified trust service identified in point (4),
   (a) the detailed description of the functional (e.g. PKI) architecture or hierarchy,
   (b) the notified documentation,
   (c) the notified CAR (ideally structured as detailed in section 4.5),

   verify that the notified TSP and the qualified trust services it intends to provide comply with the requirements laid down in the eIDAS Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide. That verification is to be performed requirement per requirement for each of the applicable eIDAS requirement with regards to the type of QTSP/QTS. For that purpose, the structure of those requirements provided in point (11) of section 4.5 of the present document can also be used as a check list for such a verification by the SB.

   The relevance and severity of each non-conformity with any eIDAS requirement[45] is to be judged by the SB as a last resort[46].

6) When the relevance and the severity of the identified non-conformity(ies) lead the SB to conclude that the notified TSP and the trust services it intends to provide as qualified do not comply with the requirements laid down in the eIDAS Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide, then the SB shall inform the trust service provider specifying the reasons for non-granting of the qualified status.

7) In the absence of non-conformities, or when the relevance and the severity of the identified non-conformity(ies) lead the SB to conclude that the notified TSP and the trust services it intends to provide as qualified do comply with the requirements laid down in the eIDAS Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide, then the SB shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) of the eIDAS Regulation (hereafter the trusted list scheme operator or TLSO) for the purposes of updating the trusted lists referred to in its Article 22(1).

8) With respect to point (7) above, the SB and the TLSO shall respect the timing constraints clarified by CID 2015/1505/EU (in particular enforcing clause 5.5.5 of ETSI TS 119 612 v2.1.1)[47] with regards to

[45] As a reminder it is important here to distinguish a non-conformity with whatever requirement from whatever standard (e.g. as potentially reported by the notified CAR) and a non-conformity with a requirement from the eIDAS Regulation.

[46] In that, the decision of the SB may overrule the CAB certification decision or non-conformity decision reported in the CAR by the CAB.

[47] *"TLSO shall ensure the consistency of the (re)-issuance of a trusted list and the actual date when a service status has been updated (e.g. granted or withdrawn), i.e. the 'List issue date and time' (clause 5.3.14), the time of signing the trusted list and the time of change. The date and time associated to the new current status of a listed service shall not*

date and time of the issuance of the trusted list and the date and time of the grant of the qualified status to the concerned trust services and as the latter will appear in the trusted list. As the QTSPs may begin to provide the qualified trust service after the qualified status has been indicated in the corresponding national trusted list, the date of the grant of the qualified status must be aligned with the date of publication of that trusted list, no back dating is allowed.

Example: A "CA/QC" service identified by the public key of an issuing technical CA whose public/private key pair has been generated (and certified) on 01.08.2016 is granted a qualified status by the SB that came internally to that conclusion on 01.11.2016 based on a notification received on 01.10.2016. The publication of the qualified status in the corresponding national trusted list can only occur (for whatever reason) on 6.11.2016. The SB and the TLSO (when they are different entities) shall make sure that the three dates regarding the date of issuance of the trusted list ('List issue date and time' - clause 5.3.14 of ETSI TS 119 612 v2.1.1), the time of signing the trusted list, and the date of granting the qualified status ('Current status starting date and time' – clause 5.5.5) shall be aligned in this example to 06.11.2016 and make sure that the updated trusted list is effectively published and available to relying parties on that same date. In no way, the date appearing in 'Current status starting date and time' (clause 5.5.5) can be back dated to an earlier date (e.g. not 01.08.2016, not 01.11.2016).

9) During the initial verification process, the SB may require additional information from the notifying TSP and from the CAB having issued the notified CAR.
10) The initial verification process should be concluded within three months meaning that when leading to a positive conclusion, the total elapsed time between the notification and the effective publication of the qualified status in the national trusted list should be less than three months. When the initial verification process would be leading to a negative decision, or would require additional information from the notifying TSP, the elapsed time between the notification and the notification of the negative decision or the request for additional information should be as short as possible and similarly less than three months. If the verification is not concluded within three months of notification, the SB shall inform the notifying TSP specifying the duly motivated reasons (see point 11 below) for the delay and the new deadline by which the verification is to be concluded.
11) During the initial verification process, the SB should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality.

be set before the date of (re)issuance of the trusted list as retroactive status change can have undesired effects to previous validations of listed services and of their outputs".

7. Supervisory body resources and organisational measures

EU Member States are not obliged by the eIDAS Regulation to have CABs established on their territory or even to have their existing NAB being able to accredit CABs on their territory. However, Article 17 of the eIDAS Regulation requires EU MS to designate a supervisory body established in their territory (or, upon mutual agreement with another Member State, a supervisory body established in that other Member State) to be responsible for supervisory tasks in their territory. Each EU MS is further required to give such a body the necessary powers and adequate resources for the exercise of those supervisory tasks (see Art.17.4).

The tasks of supervisory bodies can be grouped in different categories of activities:

- Cooperation (with other SBs - Art.17.4.(a); with data protection authorities - Art.17.4.(f), with NABs)
- Analysis of QTSP/QTS and qualified status life-cycle management
    - analysis of initial and 2-yearly CAR - Art.17.4.(b).
    - grant and withdraw of qualified status (Art.17.4.(g)).
    - auditing or requesting audits (Art.17.4.(e)) and analysing resulting ad hoc CAR.
    - monitoring deadlines for each QTS from each QTSP (e.g. 2-yearly or ad hoc CAR, request for complement of information, resolution of notified non-conformities.
    - verify the existence and correct application of provisions on termination plans (Art.17.4.(i)).
    - monitoring of QTSP/QTS activities (this may include proactive or ex post monitoring and verification of the provisions, practices and policies of the QTSP/QTS).
    - analysing QTSP/QTS provision changes notified under Art.24.2.(a).
- Information/reporting (breaches notifications to other SBs and the public - Art.17.4.(c); to data protection authorities - Art.17.4.(f); activities to EC - Art.17.4.(d).
- Management of the documentation related to the supervision activities (including their publication, e.g. as required under CID (EU) 2015/1505 with regards to the supervision scheme, Art.21.1 notification procedure and form, Art.19 breach notification, etc.).

With regards to the specific activities related to the initiation of qualified trust services, the main tasks are related to the set-up of the supervision activities and of the related documentation, as well as to the analysis of the CAR, the decision to grant or not a qualified status, the notification to the notifying TSPs of the decision and potentially of the non-conformities and/or request for additional information, the update of the national trusted list, via the trusted list body when different from the SB, when applicable.

Quantifying the resources will basically depend on the number of notifying TSPs, of notified trust services, of QTSPs and QTSs. SBs may also rely on internal resources and/or on external resources when internal resources are not sufficient.

Supervisory bodies should employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules, as well as regarding to the provision of trust services and the underlying technology, including trusted lists specifications.

Supervisory bodies or their national government may establish fees to be supported by notifying TSPs and QTSPs with regards to the notification, verification and supervision tasks they generate. Considering the notifying TSPs and QTSPs are already supporting the costs of the initial and regular conformity

assessments, those fees when applied should be reasonable, proportionate, justified and not create barrier to market entrance.

Specific attention should be paid by SB and EU MS on the potential need for taking over part or all termination activities in case of failure for the QTSP (or the expected taking over 3rd party) to correctly execute the termination plan. This may include recommendations on the set up of appropriate legislative instruments ensuring proper execution of a QTSP/QTS termination plan and in particular proper implementation of Art.24.2.(h) (e.g. in case of unscheduled termination such as bankruptcy).

8. References and bibliography

8.1 References

REF. ID	DESCRIPTION
[1]	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

8.2 Bibliography

ID	DESCRIPTION
(a)	IAS² European Commission Study – SMART 2012/0001. http://blogs.dlapiper.com/iasproject/

8.3 Relevant implementing acts

REF. ID	DESCRIPTION
(i)	Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services. OJ L 128, 23.5.2015, p. 13–15. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2015.128.01.0013.01.ENG
(ii)	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. http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015D1505
(iii)	Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 235, 9.9.2015, p. 37–41. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0006
(iv)	Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 109, 26.4.2016, p. 40–42. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D0650

Annex A: Glossary, concepts and frequently asked questions

A.1 eIDAS – What is it?

eIDAS is the acronym used to refer to Regulation (EU) No 910/2014 on electronic identification (eID) and trust services for electronic transactions in the internal market. The eIDAS Regulation is about trust, seamless user experience and convenience in online cross-border transactions.

A.2 Trusted list

A trusted list is a list including information relating to the qualified trust service providers which are established in and supervised by an EU Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in the eIDAS Regulation. Those lists have constitutive value and are the primary source of information to validate that a qualified status has been granted to a QTSP and to the QTS it provides.

Trusted lists are essential elements in building trust among electronic market operators by allowing users to determine the qualified status and the status history of trust service providers and their services.

Member States may include in the trusted lists information on non-qualified trust service providers, together with information related to the non-qualified trust services provided by them. It shall be clearly indicated that they are not qualified according to the eIDAS Regulation.

Member States may include in the trusted lists information on nationally defined trust services of other types than those defined under Article 3(16) of the eIDAS Regulation. It shall be clearly indicated that they are not qualified according to the eIDAS Regulation.

A.3 QTSP/QTS requirements and obligations

The eIDAS Regulation foresees a set of requirements and obligations for qualified trust service providers (QTSP) and qualified trust services (QTS) they provide in order to ensure a high level of security for the qualified trust services. Those obligations include in a nutshell:

- **Processing of personal data** shall be carried out in accordance with Directive 95/46/EC.
- A Trust service provider (TSP) is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation, while the **intention or negligence of a QTSP shall be presumed**, unless proven otherwise by the QTSP. When TSP informed customer in advance on limitations on the use of their services, and when such limitations are recognisable to third parties, TSP is not liable when limitations have been exceeded.
- Where feasible, services must be **accessible for person with disabilities**.
- **Implementing appropriate technical and organisational measures to manage the risks** posed to the security of the trust services they provide. Taking the latest technological developments into account, those measures shall ensure that the level of security is commensurate to the degree of risk. Measures shall be taken to prevent and to minimize the impact of security incidents and to inform stakeholders of the adverse effects of any such incidents.
- Very strict rules regarding the obligation of **notifying security & personal data breaches**.
- **Additional requirements on QTSP operations and practices**:
    - Inform the SB of any change in QTS provisioning and of intention to cease;
    - Have an up-to-date termination plan, agreed with the competent supervisory body (SB), to ensure continuity of service;

- Requirements on employed staff and subcontractors, when used;
- Sufficient financial resources and/or liability insurance, in accordance with national law;
- Inform consumers on terms and conditions, incl. on limitations on use;
- Use of trustworthy systems and products ensuring the technical security and reliability of the supported processes;
- Use of trustworthy systems to store (personal) data in a verifiable form;
- Take appropriate measures against forgery and theft of data; and
- Record and keep accessible all relevant information concerning data issued and received, even after cessation of activities.

- **Specific requirements** from the provisions laid down in the eIDAS Regulation with regards to the provision of a specific type of qualified trust service.

All those requirements must be met by the QTSP/QTS before issuing the very first qualified trust service output, e.g. before issuing the very first qualified time stamp in the case of QTSP providing qualified time stamping services.

Once granted a qualified status, the eIDAS Regulation also foresees an active supervision scheme of qualified trust service providers (QTSP) and qualified trust services (QTS) they provide by the national competent supervisory body (SB) to monitor the fulfilment of the QTSP/QTS requirements and obligations throughout their lifetime.

A.4 Service digital identity

The granularity of the identification in the national trusted lists of the technical instance of the qualified trust service to which the qualified status is granted is actually clarified by the Commission Implementing Decision (EU) 2015/1505[48]. It corresponds to the level of the "Service digital identity" field as specified in ETSI TS 119 612 v2.1.1 on which the CID relies to establish the content and define the technical specifications and formats for the national trusted lists. In a trusted list, a qualified trust service to which a qualified status is granted is identified by the public key[49] identified by the "Service digital identity" field of the corresponding trusted list service entry of a listed TSP entry. The type of qualified trust service for which the qualified status is granted is identified by the combination of the "Service Type Identifier" field and the "Additional Service Information" extension when present and further specifying the type of service.

With regards to service type identifier "TSA/QTST" URI[50], instead of assigning it (only) to time stamping units (TSUs) is it possible to assign it to a service digital identity, i.e. the public key, of an issuing CA (respectively a Root-CA) that issues (respectively under which are issued) certificates to TSUs that in turn sign time stamps. Both implementations are actually possible, namely:

- Listing a TSU public key (certificate) as "Service digital identity" of a service of type "TSA/QTST" is of course possible: any time stamp issued by such a listed TSU with a granted qualified status at the time indicated by the time stamp shall be considered as qualified), and

[48] 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 (Text with EEA relevance). OJ L 235, 9.9.2015, p. 26–36.
[49] When based on PKI public-key technology (when not based on such technology, an indicator expressed as a URI is used to identify uniquely and unambiguously the listed service).
[50] http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

- The service type identifier “TSA/QTST” URI can also be assigned to a CA public key (certificate) instead of to a TSU public key (certificate) , but in such case "O=" attribute of certificate might not match the 'TSP Name' written within TSL (there are TSPs(QTS) using TSU certificates issued by other TSPs) and this is required by ETSI TS 119 612 (5.5.3 Note 4 “With regards to X.509 Certificates that are candidates to represent a public key identifying a listed service, the TLSO shall disregard certificates for which the "O=" attribute does not strictly match the 'TSP Name' value”).

For that to be eligible, all TSUs either listed directly or signed by a CA listed as “TSA/QTST” service must reach the qualified level, all issued time stamps must be qualified and the corresponding QTSP and its QTS consisting in issuing qualified time stamps must meet the applicable eIDAS requirements.

When listing a CA with a type “TSA/QTST”, it is de facto required to have that CA issue certificates to qualified TSUs[51] only (to the exclusion of non-qualified TSUs) and to have those TSUs to issue qualified time stamps only (to the exclusion of non-qualified time stamps) as in the context of time stamps it would be much more difficult than in the context of certificates to distinguish between those types of time stamps when the listed CA issue certificates for both types of TSUs, actually:

- Best practices and relevant standards require the use of time stamping policy OID indication in the time stamp but there is only one field allowing one single OID and this can be any proprietary OID or the “best practices level OID” defined by ETSI EN 319 421. ETSI EN 319 422 defines a time stamp extension for where to place a "QtstCompliance" statement (by analogy with the QcCompliance statement for qualified certificates) but it is not mandatory and it is not commonly used in existing implementations. ETSI EN 319 421 further requires that when a TSU issues qualified time stamps, that TSU shall not issue non-qualified time stamps and TSA should use separate TSU for issuing qualified and non-qualified time stamps.
- In the eIDAS Regulation,
    - there is no requirement to indicate in the time stamp itself that it was created as qualified, and
    - there is no requirement to implement or comply with any standard.
- There is, under the current TL specifications, no possibility for the TLSO in a “TSA/QTST” entry of a trusted list to further qualify some set of time stamps for being labelled as qualified or not-qualified when issued under the same TSU or the same (root) CA issuing TSU certificates.

So when a TSA/TSP wants to issue both qualified and non-qualified time stamps, having separate dedicated TSUs (creating exclusively either qualified or non-qualified time stamps) and grouped under two separate dedicated CAs (either signing qualified TSUs or non-qualified TSUs) would be a must when using the approach of listing the CA in the TL as “TSA/QTST” type of service.

Actually, when an issuing CA is not signing exclusively qualified TSUs that issue qualified time stamps exclusively, then that issuing CA cannot be used as Service Digital Identifier (Sdi) in a “TSA/QTST” entry and all corresponding qualified TSUs issuing exclusively qualified time stamps must be listed separately.

A.5 What does Regulation (EC) 765/2008 bring as advantages to the SBs and to the TSPs?

Regulation (EC) 765/2008 ensures the equivalence of the level of competence of conformity assessment bodies (CABs) with the aim of facilitating mutual recognition and of promoting the overall acceptance of accreditation certificates and conformity assessment results issued by accredited bodies.

[51] That same CA would also be entitled to issue QCs, in theory, when meeting the applicable requirements.

All EU MS have one single national accreditation body (NAB) appointed under Regulation (EC) 765/2008, member and signatory of the EA multilateral agreement[52]. Accreditation through NABs that are signatories of the EA MLA provides a further level of confidence that the accredited CABs are independent, competent, and that they work in a consistent way.

Each NAB is subject to routine and rigorous evaluations by peer evaluation teams in order to verify continuing compliance with Regulation (EC) 765/2008 and the international standard for accreditation bodies (ISO/IEC 17011). Each NAB has an obligation to inform the other NABs with regards to the conformity assessment activities in respect of which it operates accreditations and of any changes thereto. To that end, it also takes part in regular technical discussions with other NABs to harmonise their activities. NABs demonstrating conformity with harmonised standards by successful peer evaluation (Art.10) are presumed to fulfil requirements of Regulation (EC) 765/2008 (Art.8).

Accreditations granted by any Regulation (EC) 765/2008 - compliant NABs are deemed equivalent for a considered conformity assessment scheme.

NABs manage the accreditation certificate life cycle for each CAB they have granted an accreditation: i.e. they monitor the accredited CABs, restrict / suspend / withdraw accreditation certificates when required.

NABs are permitted to operate across national borders. In theory, CABs must be accredited by the NAB of the country in which they are established but in the event the NAB does not provide services for the expected accreditation scheme then a CAB may request accreditation services from an EA MLA signatory NAB from another country than the one in which the CAB is established.

Conformity assessment attestations (e.g. certifications) issued by all CAB accredited by Regulation (EC) 765/2008 compliant NABs are deemed equivalent, for a considered conformity assessment scheme (e.g. certification scheme)[53]. This means that a TSP, either without qualified status and intending to start providing QTSs or being a QTSP providing QTS, that is required to provide its national SB with a CAR issued by an accredited CAB, can choose whatever CAB from whatever EA MLA signatory country that has been accredited under a valid eIDAS accreditation scheme for obtaining such a CAR. The competent SB cannot reject the eligibility of the notified CAR because it has not been provided by a CAB established or accredited in the territory for which the SB is competent.

A.6 Trust services defined by the eIDAS Regulation

In its Art.3.16, the eIDAS Regulation defines a 'trust service' as an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services.

A.7 Which are the qualified trust services defined by the eIDAS Regulation?

[52] NAB-Malta signatory in testing except ISO 15189. NAH, the new HU NAB full EA member with effect from 1 April 2016 applied for the EA MLA signatory status and the peer evaluation of NAH is ongoing.
[53] See Art.11.2 of Regulation (EC) 765/2008.

Only those trust services listed in Art.3.16 of the eIDAS Regulation for which there are applicable requirements in the Regulation can benefit from the qualified status. eIDAS regulates the following nine qualified trust services:

1. **The creation of qualified certificates for electronic signatures**

   Certificates for electronic signature are electronic attestations which link electronic signature validation data to a natural person and confirm at least the name or the pseudonym of that person. Since 1 July 2016, an electronic signature can only be used by a natural person to sign, i.e. mainly to express consent on the signed data/document. This represents a significant difference from the eSignature Directive 1999/93/EC regime, where an electronic signature, which could be used by legal persons, was defined as a means of authentication. Under the eIDAS Regulation, the entity who creates an electronic signature (the so called signatory) will be a natural person. Therefore, certificates for electronic signature cannot be issued to legal persons anymore. Instead legal persons can use certificates for electronic seals (see below).
   A qualified electronic certificate for electronic signatures is an essential element for a signatory to create qualified electronic signatures that shall have the equivalent legal effect of a handwritten signature all over the EU.

2. **The creation of qualified certificates for electronic seals**

   As explained above, since 1 July 2016, legal persons cannot create legally valid (qualified) electronic signatures anymore and cannot be issued (qualified) certificates for electronic signatures. Instead legal persons can use certificates for electronic seals, which are electronic attestations that link electronic seal validation data to a legal person and confirm the name of that person. The aim of an electronic seal is not to sign but to serve as an evidence that an electronic data/document was issued by a legal person, ensuring certainty of the data/document's origin and integrity.
   A qualified electronic certificate for electronic seals is an essential element for a legal person to create qualified electronic seals that shall enjoy, all over the EU, the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

3. **The creation of qualified certificates for website authentication**

   Certificates for website authentication are issued to ensure the users (in particular citizens and SMEs) that behind the website there is a legal or natural person identifiable by trustworthy information.
   The Regulation sets clear requirements for qualified website authentication certificates to be considered trustworthy together with obligations for qualified trust service providers of such qualified certificates with regard to the security of their operations, their liability and their supervision regime. As a consequence, the Regulation ensures transparency regarding the quality of the service offered to users, accountability of providers with regards to the security of their services, trustworthiness of the data associated to qualified authenticated websites and technological neutrality of services and solutions.

4. **Qualified preservation service for qualified electronic signatures**

   Such a qualified trust service aims to ensure the long-term data preservation, in order to ensure the legal validity and trustworthiness of qualified electronic signatures over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

5. **Qualified preservation service for qualified electronic seals**

   Such a qualified trust service aims to ensure the long-term data preservation, in order to ensure the legal validity and trustworthiness of qualified electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

6. **Qualified validation service for qualified electronic signatures**

   Validation of electronic signature is an ancillary service to electronic signatures whose process aims to confirm the validity of an electronic signatures.
   Qualified validation services for qualified electronic signatures entail the verification by a qualified trust service provider that the requirements of the eIDAS Regulation are met by a qualified electronic signature in order to confirm its validity.

7. **Qualified validation service for qualified electronic seals**

   Validation of electronic seal is an ancillary service to electronic seals whose process aims to confirm the validity of an electronic seals.
   Qualified validation services for qualified electronic seals entail the verification by a qualified trust service provider that the requirements of the eIDAS Regulation are met by a qualified electronic seal in order to confirm its validity.

8. **Qualified electronic time stamps services**

   Electronic time stamps are issued to ensure the correctness of the time linked to data/documents. Qualified electronic time stamps shall enjoy, all over the EU, the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

9. **Qualified electronic registered delivery services**

   By relying on a qualified electronic registered delivery service, one will benefit, all over the EU, from the presumption of the integrity of the registered data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of the sending and the reception indicated by that qualified trust service.

The Regulation sets clear requirements for all such qualified trust services to be considered trustworthy together with obligations for their qualified trust service providers with regard to the security of their operations, their liability and their supervision regime.

A.8 EA rationale for selecting ISO/IEC 17065 & ETSI EN 319 403 as the CAB accreditation framework for TSP/TS assessments

It should be noted as well that the EA promoted accreditation scheme requires CABs to be *certification bodies*, and not simply inspection bodies or laboratories as CABs are required to certify the conformity of QTSPs/QTSs against the applicable requirements of the eIDAS Regulation.

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

> *EA members unanimously selected ISO/IEC 17065 as the best option as basis for the accreditation of CABs in the context of conformity assessments of TSPs and trust services they provide, and in particular assessment of QTSPs/QTSs. EA experience is that ISO/IEC 17020 is not considered*

appropriate to assessment of conformance of requirements for the management system of the TSP, and it is considered that a review of the security management system of the TSP constitutes an important part of a TSP audit.

Also, ISO/IEC 17020 does not impose a continued assessment by following deviations of the use of certification brands. Inspection processes tend to review the status of the items being inspected at a point in time whereas the requirements for a TSP need a more long term, continuous assessment as provided by a certification scheme. The issue of certification includes requirements for regular surveillance activities as well as specific requirements for ongoing quality and service improvement.

On their own ISO/IEC 27006 and 17021 are not considered sufficient to cover assessment of specific service requirements. However, ISO 17065 was specifically designed to be extended to incorporate requirements from 17021, but the opposite is not true as ISO/IEC 17065 requirements do not fit well into ISO/IEC 17021.

The industry requirement for public trust services, such as reflected in the CA/Browser Forum guidelines and in other national schemes for non-qualified trust services, strongly supports a clear indication of the technical compliance to good practice in industry. The aim of the ETSI EN 319 403 conformity assessment is also to allow an assessment of conformance to industry good practices as well as that the technical requirements of the Regulation are met. ETSI/CEN consider that any scheme which falls short of assessment against industry good practice will bring the acceptability of qualified trust services into question.

There is no inconsistency between a certification by an accredited CAB and the SB having final decision on whether or not the (Q)TSP/(Q)TS meets the eIDAS requirements. Art.3.18, referring to Regulation (EC) 765/2008, makes it possible the CAB to be a certification body, or an inspection body, or a laboratory, with the requirement that the CAB must be accredited for its competences to assess QTSP/QTS against all requirements of eIDAS. It is worth emphasising that the final decision is in the hands of the SB. The latter may rely upon the information provided by the (Q)TSP and in particular the CAR but it is equally entitled to request further information and it may take duly justified decision (e.g. applying good principle of administration and principle of proportionality) that goes against the conformity assessment report.

It is worth stressing as well that the annual surveillance audit that may be a requirement coming from the accreditation/certification scheme under which CAB is accredited and (Q)TSP/(Q)TS are audited (e.g. §7.9 of ISO 17065 and EN 319 403) is not a requirement from the eIDAS Regulation. Neither is the requirement for a continued assessment by the CAB. Those continued assessments and annual surveillance audits are no substitution of ex post supervisory activities of supervisory bodies.

A.9 Is the lack of implementing acts adopted pursuant to Art.20.4 of the eIDAS Regulation an issue?

It should be noted that the implementing acts foreseen in Art.20.4 are not mandatory but optional. There is no obligation for the EC to establish such acts. The provisions of the eIDAS Regulation are supposed self-sufficient in order to ensure the applicability of the legal framework. As for all optional implementing act, those Art.20.4 acts are deemed related to non-essential elements of the Regulation that are not substantial for the Regulation to work. The need to adopt them must be assessed on a case-by-case basis in the light of several principles including:

- **The eIDAS framework consistency**: in the present case adopting Art.20.4 implementing acts would require to ensure its consistency with other implementing acts granting QTSPs/QTSs with a presumption of compliance with some legal provisions.
- **Taking into account stakeholders/market needs**: evaluating stakeholders/market's demands and needs, potential barriers hampering the adoption and take-up of eIDAS.
- **Favouring a non-regulatory approach, a co-regulatory approach, and a development under other regulatory frameworks**: In this case, as the implementation of an eIDAS accreditation scheme may be ensured under the framework of Regulation 765/2008/EC, as being set up by EA, the implementing act foreseen in Art.20.4 may not be needed. Furthermore, adopting a secondary act means codifying a given technological approach that may quickly become obsolete, requiring a revision of the adopted act.
- **Availability and adequacy of standards**: Before being able to reference a standard, such a standard must be available. However, the availability of a given standard or technical specifications does not automatically entail an obligation for the Commission to list it in an implementing act. Moreover, once standards become available, it is critical to assess their compliance with the requirements set in the Regulation before considering a possible reference in secondary acts. Such a referencing will also be scrutinized in the light of the other principles above.

Art.20.4 only allows the EC to reference standards for the accreditation of CABs under eIDAS, for the CAR resulting from the audit confirming that the QTSP/QTS fulfil the eIDAS requirements and for the auditing rules under which CABs will carry out their conformity assessment of the QTSP/QTS. It does not empower the EC to specify the requirements related to these topics. In particular, the referencing of the ETSI EA promoted scheme would provide that QTSP/QTS audit criteria ("third layer of the scheme") to be standardised in such a way that:

- The resulting CAR issued by accredited CABs aims to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in the eIDAS Regulation.

- It consists of one or more separate standards, "outcome based" (see 4.4.1), mapping audit criteria built as control objectives and controls, against the requirements of the Regulation per type of qualified trust service. Those criteria shall be used by accredited CABs as a basis for establishing the conformity assessment report to be issued by them, confirming that the QTSP/QTS they assess fulfil all applicable requirements of the Regulation.

  Those criteria defined in an "outcome based" approach could leverage once assessed as conform to the eIDAS Regulation, on the check lists specified by or in the context of relevant available standards (e.g. the check list from ETSI EN 319 411-2 with regards to QTSPs issuing qualified certificates); it should however be clear that those criteria are for use by CABs as a method to produce a conformity assessment report on the conformity of the audited QTSPs/QTSs and shall not presuppose or require QTSPs/QTSs to comply with the standards from which they are derived. QTSPs/QTSs are free to implement such standards, any other standard or no standard at all. Current CEN/ETSI standards addressing QTSP and QTS related specifications, including the ETSI EN 319 4x1 series and any other relevant standards, can be used by TSPs on a voluntary basis but cannot be made (de facto) a mandatory requirement for being granted a qualified status.

- Whenever compliance with part of the applicable eIDAS requirements would be deemed satisfied by compliance with a sub-referenced standard, this would be acknowledged provided the

conformity with such a sub-referenced standard has been assessed and confirmed by an eIDAS accredited CABs.

Currently no such QTSPs/QTSs audit criteria outcome based standard conformity exists and no other conformity assessment scheme owner has undertaken the standardisation of a competing eIDAS compliant scheme. It would be recommended that once a sufficient maturity in the effective criteria used to accredit CABs either defined by CABs themselves, by SBs or by any other competent body, the European Commission could ask CEN/ETSI to leverage on that experience to derive an appropriate standard.

This does not prevent the eIDAS CAB accreditation scheme and corresponding conformity assessment schemes to be used for accreditation of CABs against specific set of TSP oriented standards so that QTSPs/QTSs can benefit from confirmation (e.g. certification) of conformity against any of such specific standards. Such schemes may also be used to additionally confirm (e.g. certify) compliance with standards for use out of the context of the eIDAS Regulation (e.g. CA/Browser Forum and its associated industry) but also for attesting compliance with standards possibly referenced in the future in (optional) eIDAS secondary legislation.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Catalogue Number TP-06-16-340-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-189-2
DOI: 10.2824/238163