THE EU CYBER SECURITY AGENCY

GUIDELINES ON SUPERVISION OF v ¦ ! [LCL95 ¢w ¦ {¢ {9R±L/9{

Technical guidelines on trust services

DECEMBER 201T

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: 978-92-9204-190-8
DOI: 10.2824/361221

Table of Contents

Notice: All Annexes mentioned in this document, refer to the corresponding numbers of Annexes included in the document “Guidelines on Initiation of Qualified Trust Services”.

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
CSP	Certification Service Provider
DDF	Due Date File
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].

It is possible to use those trust services as well as electronic documents as evidence in legal proceedings in all EU Member States contributing to their general cross-border use. Courts (or other bodies in charge of legal proceedings) cannot discard them as evidence only because they are electronic but they 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 national eID and electronic 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 electronic 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 the national level. It also creates an EU wide internal market for electronic trust services by ensuring their recognition and workability across borders and are considered 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 benefit 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 evidence, 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 Annex A.1 or Art.3.16 of the eIDAS Regulation for the definition of trust services.

Without undergoing an identity verification based on physical presence, but by using a 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 the receipt indicated by that qualified trust service.

1.3 Specific role of the qualified trust services

To further enhance the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, 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. Based on the notified information (including the report of such an audit and any additional information requested from TSP which was necessary to verify compliance with the requirements laid down in eIDAS regulation), the competent SB will formally verify whether the

[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).

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 is granted a qualified status separately for each type of qualified trust service covered by the eIDAS Regulation. For example, a QTSP qualified for supplying 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 provision of qualified electronic time stamps published explicitly in the national trusted list before issuing qualified time stamps in addition to the provision 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 the rules of the Commission Implementing Regulation (EU) 2015/806.[6] Basically, this secondary legislation defines the form, colour and size of the EU trust mark. It also sets the obligation to clearly indicate the qualified service that the EU trust mark pertains to. However, it allows for associating the EU trust mark with other graphical or textual elements provided that certain conditions are met.[7]

The use of the EU trust mark, which is voluntary, aims to foster transparency of the market and help consumers distinguish between qualified trust services and non-qualified ones. Once granted a qualified

---

[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 Content Service Provider shall not be considered as a QTSP from 2 July 2017.

[5] See Annex A.7 for further details. All Annexes mentioned in this document, refer to the corresponding numbers of Annexes included in the document "Guidelines on Initiation of Qualified Trust Services".

[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.

status, QTSPs and their QTSs have the obligation to pass two-yearly conformity assessments by an accredited CAB, confirming that the QTSP and the QTSs they provide fulfil the requirements laid down in the Regulation. The resulting conformity assessment report (CAR) has to be submitted the competent supervisory body. Competent supervisory bodies are also allowed themselves, at their own discretion and at any time, to audit any QTSP/QTS for which they are competent or to request an accredited CAB to perform an ad hoc audit.

Figure 1 EU trust mark for qualified trust services

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]. The present document proposes "Guidelines on Supervision of Qualified Trust Service Providers" pursuant to Art.20 of the eIDAS Regulation. The target audience of the document are trust service providers (including individuals, businesses and public administrations) who intend to start providing or are currently providing qualified trust services and those Member States supervisory bodies designated to carry out supervisory activities under the eIDAS Regulation.

The objective of the document is to support QTSPs providing qualified trust services and supervisory bodies in their respective tasks and duties during the supervision and during the verification of compliance with the eIDAS Regulation and the management of the qualified status through the publication of an updated national trusted list, when applicable. The guidelines cover the procedures and formats for the supervision of a qualified trust service. The guidelines shall enable supervisory bodies to establish the rules, requirements and recommendations for a TSP to manage the life cycle of the supervision of the qualified trust services it provides and to continue to meet the requirements of the eIDAS Regulation until and beyond the termination of those services.

This document is organised to provide:

- Recommendations to QTSPs and SBs with regards to the supervision and the life cycle management of the qualified status for QTS (section 2).
- An overview of the eIDAS Regulation provisions relating to the supervision of QTSPs (section 3).
- The provisions on the supervision process flow and the underlying activities (section 4).
- Recommendations to SBs on the cooperation with other EU MS SBs (section 5).

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

2. Guidelines on Supervision 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 bodies (SBs) 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**. From there, the supervision scheme covers the full life cycle of each QTS and each QTSP, from its genesis until its termination.

2.2 Supervision of Qualified Trust Service Providers

Once a qualified status is granted, the supervision process flow can be split into the following steps of related supervisory activities, as sketched below, for each QTS at the level of granularity addressed in the national trusted list:

- The **detection or notification of events**: Those events will actually condition the next steps in the supervision process; each of those events may lead the competent SB to withdraw the qualified status of the corresponding QTSP/QTS:
    - 2-yearly anniversary from the initial qualified status grant
    - 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 **need for additional evidence**: This can consist in

  - The SB requesting additional information or evidence from the QTSP
  - The SB conducting an ad hoc audit
  - The SB requesting a CAR from an accredited CAB.
- The **verification of compliance**: based on the event data and the potential additional evidence, the SB will conduct a verification of the compliance of the concerned QTSP and its related QTSs. During that step, the SB may also face the need for additional evidence.
- The **decision on a status change**: based on the results of the compliance verification, the SB may decide to keep the qualified status unchanged (granted) or to withdraw the previously granted qualified status. Once the qualified status has been withdrawn from a QTS and hence from its QTSP for the provision of that QTS, the corresponding TSP and trust service are "sent back" to the initiation process if the TSP wishes to be granted again a qualified status for that specific trust service.

This document proposes guidelines[9] to SBs and (Q)TSPs on the supervision of qualified trust services pursuant to Art.20 of the eIDAS Regulation. They come in addition to the recommendations provided in the context of the initiation of qualified trust services as provided in the companion document "Guidelines on Initiation of Qualified Trust Services"[10].

[9] 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
[10] "Guidelines on Initiation of Qualified Trust Services", https://www.enisa.europa.eu/topics/trust-services/guidelines/

2.3 Recommendations for Supervisory Bodies

The following are **recommendations** for supervisory bodies in the context of the supervision of QTSP:

SB.1 – Supervisory body resources

(a) Make sure to be given the necessary powers and adequate resources and organisational measures for the exercise of its tasks [11].
(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. With regards to the supervision activities in the context of the life cycle management of the qualified status of a QTSP/QTS, see section 3 of this document for further guidance on the handling and detection of relevant events, the assessment of the need for additional evidence, the verification of compliance and the decision on status change and its impact on the national trusted list.
(c) In the context of Art.17.4.(i) of the eIDAS Regulation, SBs should verify the existence and the correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with Art.24.2.(h)[12].

SB.2 – Interactions with QTSPs

(a) SB should be approachable by (candidate) QTSPs as part of the initiation process in order to ensure a smooth and transparent process.
(b) Besides the CID (EU) 2015/1505 requirement[13] on the publication of specific information on the underlying supervision scheme, SBs should publicize information about the supervision process.

SB.3 – 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.4 – "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 QTSP, with a view to facilitating the verification of the correct accreditation of the selected CAB to carry out eIDAS QTSP/QTS assessments.

---

[11] To this extent, follow recommendations provided in section 2 of the companion ENISA report "Guidelines on Initiation of Qualified Trust Services".
[12] For more details, refer to ENISA report on "Guidelines on Termination of Qualified Trust Services", https://www.enisa.europa.eu/topics/trust-services/guidelines/
[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 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 3.3 of this document for further guidance.

SB.5 – QTSP/QTS audit criteria & the structure of the CAR

(a) Both for conducting Art.20 supervision activities and for verifying the eligibility of CABs and CARs, make sure that QTSP/QTS are assessed for compliance against the applicable requirements of the eIDAS Regulation in accordance with the scope of the required assessment.
(b) Make sure and verify that the CAR explicitly confirms and bears sufficient information demonstrating that the assessed QTSP/QTS fulfil the applicable requirements of the eIDAS Regulation.

SB.6 – Procedures and means for reporting security and personal data breaches

(a) The SB should establish and make available to TSPs, including QTSPs, the applicable procedures and means for reporting Art.19.2 security and personal data breaches. In particular, the SB should provide guidance on identifying and analysing incidents and vulnerabilities, on determining how significant their impact in on the TSP, its services and personal data maintained therein, what data needs to be reported and a template of the report.
(b) The SB shall also provide simple facilities to the reporting TSP to ensure the confidentiality of the reported data.
(c) SBs should refer to the guidance and tools provided by ENISA as part of the Art.19 committee activities.[14]

SB.7 – Communication of the qualified status change and national trusted list update

(a) The SB and the TLSO shall conform to CID 2015/1505/EU. See section 3.4 of this document for guidance on the granularity of the qualified status assignment.

SB.8 – Cooperation with other EU MS SBs under Art.18 of the eIDAS Regulation

(a) Collaboration under Art.18 with other EU MS SBs is strongly recommended when a (Q)TSP activities and operations related to the provision of QTS are spread across national borders. See section 4 for further guidance.
(b) Since it may be considered impossible to report every change in the provision of QTSs under Art.24.2.(a), SBs should cooperate to set-up mechanisms to classify such changes, e.g. in function of their relevance and impact on the compliance of the QTSP/QTS with the eIDAS Regulation.
(c) SBs should cooperate to the set-up a common template for the annual reporting on their supervisory activities as foreseen in Art.17.6 of the eIDAS Regulation. ENISA report entitled" Article 19 Incident Reporting" has prepared an Incident Reporting Framework for eIDAS Article 19 in consultation with the members of the expert group and reviewed by the private sector and the Forum of European Supervisory Authorities for Electronic Signatures (FESA). Based on this document, ENISA has developed an on-line tool (CIRAS-T) to facilitate the procedure.

[14] See "Article 19 Incident Reporting", https://www.enisa.europa.eu/publications/article19-incident-reporting-framework.

(d) Whenever the SB is notified or identifies events that may or will trigger specific supervisory activities with regards to the QTSP/QTS for which another EU MS SB is competent for its supervision, the SB should inform the concerned foreign SBs without delay.

SB.9 – 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 their 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 supervison of QTS:

TSP.1 – Provision of QTS as a QTSP

(a) With regards to the supervision activities in the context of the life cycle management of the qualified status of a QTSP/QTS, it is highly recommended, if not crucial, for QTSPs to continuously manage and update a consolidated deadline schedule and supervisory activities planner (hereafter referred to as the "due date file" or DDF).
(b) This DDF should be designed to provide a complete overview of all the deadlines related to each and every QTS a QTSP has been granted a qualified status. Those deadlines will relate to the planned supervisory steps, events and tasks the supervised QTSs must undertake. The DDF should also allow for setting alarms sufficiently before the occurrence of those deadlines and for those alarms to be communicated to people in charge.
(c) This DDF should include as well annual surveillance activities or re-audit when applicable from the selected conformity assessment scheme applied by the selected eIDAS accredited CAB, even if the conduction of such surveillance activities is not a requirement stemming from the eIDAS Regulation. The results of such surveillance audits should nevertheless be reported to the competent SB.
(d) Hence it is highly recommended to the QTSP to synchronize the (Art.24.2.a) change notification and the regular surveillance and supervision mechanisms, with regards to both the CAB and its nationally designated SB, e.g. in order to undertake conduction of possible necessary re-assessment of changes at the time of the next regular surveillance or 2-yearly supervision audit.

TSP.2 – Understanding the granularity of the identification of a trust service to which a qualified status is granted

(a) 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 the present document, to identify when they are required to notify the initiation of a new qualified trust service and when they actually need to notify any change to an existing qualified trust service or that existing service being subject to routine supervision and 2-yearly audits.

TSP.3 – Up-to-date policies, practices, procedures, process and guidelines

(a) QTSPs in order to be granted a qualified status for the provision of QTS(s) should constantly evaluate the risks, design, test, deploy, re-evaluate the risks, redesign, retest, re-implement, etc.,

the organisational, physical and technical implementation of those qualified trust services, as well as document and keep up-to-date their corresponding practices, policies, procedures, processes and documentation in line with the requirements laid down in the eIDAS Regulation.

(b) For that purpose, they should first consider the publication of the specifications by the competent supervisory body (SB) of the specifications of the applicable supervision scheme and related QTSP/QTS requirements. In particular, they should keep in mind that the purpose of the supervision is to ensure that they and the QTS (s) they provide fulfil the requirements laid down in the eIDAS Regulation.

(c) 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.4 – Adoption of standards

(a) 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 at enabling a compliant implementation that meets the eIDAS Regulation requirements. ETSI TR 119 000 gives an overview over ETSI/CEN standards that could 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.

(b) When QTSPs intend to provide a QTS that additionally meets requirements in a non-eIDAS application domain, provided those requirements are not in contradiction with the eIDAS requirements for QTSP/QTS, they may be required to comply with specific standards or normative requirements. 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.

TSP.5 – Selection of CABs

(a) QTSPs 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 3.3 of this document).

(b) 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 certify 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).

[15] ENISA report, "Recommendations for TSPs based on standards", https://www.enisa.europa.eu/topics/trust-services/guidelines/

(c) Follow recommendations of section 3.3 of this document with regards to the recommended structure and content of CARs.

TSP.6 – Participation to ad hoc fora

(a) QTSPs are encouraged to participate to ad hoc fora and cooperate with other QTSPs with regards to the implementation of best practices. Such fora include ENISA TSP Forum, ACAB-c, the eIDAS Observatory, ETSI/CEN ad hoc standardisation technical bodies, PKI Fora, etc.

TSP.7 – Interactions with competent SB

1. In order to allow for an efficient initiation and supervision 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.

3. eIDAS Regulation provisions related to the supervision of QTSPs

3.1 Supervisory bodies

Art.17.1 of the eIDAS Regulation requires Member States to designate a supervisory body established in another Member State upon mutual agreement with that Member state. Today, all EU MS have designated such a body established in their territory.

That body shall be responsible for supervisory tasks in the designating Member State (Art.17.2) and to that extent each EU MS must make sure that it will be given the necessary powers and adequate resources for the exercise of its tasks (Art.17.1).

The role of the supervisory body is further specified by Art.17.3 and includes the supervision of QTSPs established in their territory, to ensure through ex ante and ex post supervisory activities that those QTSPs and the QTSs that they provide meet the requirements laid down in the eIDAS Regulation. Art.17.4 lists a set of specific tasks amongst those of the SBs:

(a) to cooperate with other supervisory bodies and provide them with assistance in accordance with Art.18.
(b) to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1).
(c) to inform other supervisory bodies and the public about breaches of security or losses of integrity in accordance with Article 19(2).
(d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article
(e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2).
(f) to cooperate with data protection authorities, in particular, by informing them without undue delay about the results of audits of qualified trust service providers that appear to have been involved in a breach of personal data protection rules.
(g) to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21.
(h) to inform the body responsible for the national trusted list referred to in Article 22(3) about its decisions to grant or to withdraw qualified status, unless that body is also the supervisory body.
(i) to verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2).
(j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation.

3.2 QTSP/QTS supervision

The legal obligations related to the supervision of QTSPs/QTSs are also to be mainly derived from requirements of Art.20 as listed here after:

- *Art.20.1. - Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.*
- *Art.20.2. - Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.*

- *Art.20.3. - Where the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service 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). The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.*

Furthermore, Art.24.2.(a) requires a *qualified trust service provider providing qualified trust services to inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities*.

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,*[16,17] *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 introduce any implementing act with regards to the conformity assessment 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

[16] 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.
[17] See Annex A.5 for what Regulation (EC) 765/2008 brings as advantages to the SBs and to TSPs.

comply with a given standard or a given business/technical model. QTSP/QTS are free to choose their own way of devising an implementation that fulfils the eIDAS requirements, be it operationally, organisationally or technically.

3.3.1 eIDAS compliant accreditation schemes for CABs

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

The resulting conformity assessment report that is 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 that the assessed QTSP/QTS fulfils all the applicable requirements of the eIDAS Regulation (when this is the case).

Provided the above requirements are met, it is a fact that it lies 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.

The accreditation of CABs, in accordance with Regulation (EC) No 765/2008, is the exclusive competence of national accreditation bodies (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.

In practice, in order to meet the requirements of the eIDAS Regulation, the accreditation of the CAB requires an evaluation by the competent NAB based on an "eIDAS" conformity assessment scheme[18] and of the competence of the CAB employing such a 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.

Such an eIDAS conformity assessment scheme may be defined by the CAB itself, the EU MS supervisory body, or any other body possessing the necessary technical competence. It is worth emphasising that the final decision regarding the verification of the conformance of a QTSP/QTS with the requirements of the eIDAS Regulation 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 a duly justified decision (e.g. applying good principle of administration and principle of proportionality) that goes against the conformity assessment report

See section 4.4 of the companion document "Guidelines on Initiation of Qualified Trust Services" for further discussion on the different implementations of eIDAS compliant accreditation schemes for CABs, including the ETSI 319 403 accreditation scheme for TSP/TS promoted at EU level by the European co-operation for Accreditation (EA) and alternatives schemes.

[18] Such a scheme identifies the requirements on the CAB, the requirements on the auditing rules under which the CAB will carry out its 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.

3.3.2 Structure and content of CAR

It is ultimately the supervisory body (SB) to which the CAR is notified by the assessed QTSP that will take the decision to grant or withdraw the qualified status to the assessed QTSP/QTS. Consequently the notified 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.[19] It is not regarded as suitable that the SB that has the obligation to verify the compliance of the (Q)TSP/(Q)TS with the eIDAS Regulation will solely base its decision on a "yes/no" CAR.

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 bears sufficient information to demonstrate that the TSP/TS complies with the requirements laid down in the eIDAS Regulation, and in particular, with the requirements for QTSP/QTS.

Recommendations on the structure and on the content of the CAR referred to in Articles 20.1, 20.2 and 21.1 of the eIDAS Regulation can be found in section 4.5 of the companion document "Guidelines on Initiation of Qualified Trust Services".

3.4 Granularity of qualified status assignment

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 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 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 providing qualified certificates for electronic signatures is not to be considered as qualified for providing any other qualified trust service, including the issuing of qualified certificates for electronic seals or for website authentication, or the supply 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[20]. 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 to 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[21] 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

[19] Further evidence demonstrating the compliance of QTSP/QTS with the requirements of the eIDAS Regulation may be included by reference to other reports, such as reports of audits against technical standards, which contain detailed and herewith sufficient information for the SB to judge the QTSP/QTS conformity.
[20] 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.
[21] 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).

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 the service[22].

On the other hand, the initiation process foreseen by Art.21 of the eIDAS Regulation is required to be undergone by a TSP not already having a qualified status for providing 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. 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 Certification Service Providers (CSP) 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 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 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 significantly changing anything else with regards to the provision of their services that benefit from the Art.51 measures should not need to go through the Art.21.1 initiation process.

Of course, in all cases of applying Art.24.2.(a), a "classification" of changes should be considered in practice, i.e. an assessment of how "significant" the change is 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 SB (contrary to the termination, where the intention to cease activities is required to be notified before cessation). Nevertheless, it is recommended to the QTSP to notify them before their implementation so that the supervisory body is able to approve (or make comments / indicate possible eIDAS non-conformities on) significant changes before they are implemented.

[22] 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.

See also Annex A.4 (of the document "Guidelines on Initiation of Qualified Trust Services") for guidance on the use of the "Service digital identity" field in the trusted list with regards to qualified trust services and section 3.4 of the companion document "Guidelines on Initiation of Qualified Trust Services" for examples.

3.5 Standards and best practices

As previously stated, neither the business model, nor the technical model can be imposed on QTSPs. Similarly, QTSPs cannot be forced to follow any specific standard for the QTS they provide. 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/QTSs.

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

- CABs, NABs, and SBs in the establishment of effective eIDAS QTSP/QTS criteria, related control objectives and controls that will be used for assessing QTSP/QTS against the eIDAS Regulation.
- TSPs when designing, implementing and demonstrating 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 for 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 establish conformity assessment schemes aimed at assessing the 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 assessing their compliance with the requirements set in the Regulation. Once the corresponding 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[23] gives an overview over ETSI/CEN standards that could 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[24]. It concluded that the analysed standards usually cover some requirements in part or whole

[23] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".
[24] ENISA report, "Recommendation for TSPs based on Standards", https://www.enisa.europa.eu/topics/trust-services/guidelines/.

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 a 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[25] 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 their 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.

[25] 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 stone of the eIDAS pyramid of trust

The supervision model[26]of qualified trust service providers (QTSPs) and of the qualified trust services (QTSs) they provide is the foundation of the 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 2.

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 the trustworthiness of the qualified trust services it provides.

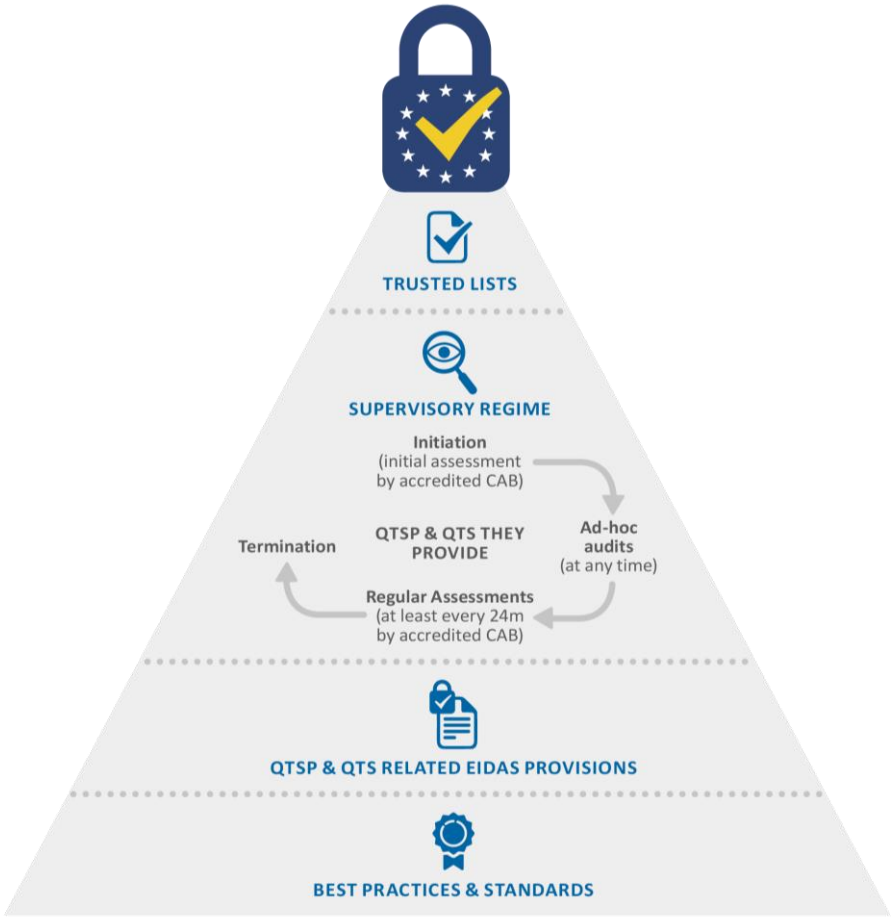

Figure 2 eIDAS Regulation building trust in the online environment (Source IAS² - updated)

[26] Going through a pre-authorisation assessment process is required before a TSP, without qualified status, is allowed to provide any QTS. Once being granted a qualified status, the QTSP and the QTS it provides are supervised until their termination on the basis of regular re-assessments and on potential ad hoc assessment on the initiative of the competent supervisory body or as a result of third party notifications or complaints.

This EU trust mark is not just another quality logo without any trust foundation. As illustrated in Figure 2 above, the eIDAS Regulation explicitly sets up a consistent set of quality/security requirements and obligations for QTSs/QTSPs. 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 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 a national supervisory body in each EU Member State. It 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 conformity assessment report (CAR) issued by an accredited conformity assessment body (CAB) confirming that the QTSP and the QTSs it intends to provide meet the requirements laid down in the Regulation.
- It determines that SBs are responsible to verify the compliance of the submitted CAR and any additional submitted information with 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 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 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 in a trustworthy manner.

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. For verification purposes, QTSPs using the EU trust mark for qualified trust services are obliged to provide a link to the corresponding trusted list in close proximity to the EU trust mark.

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 a number 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 supervision process flow

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. Guidance to SBs and to (Q)TSPs on the initiation step are provided in the companion document "Guidelines on Initiation of Qualified Trust Services".

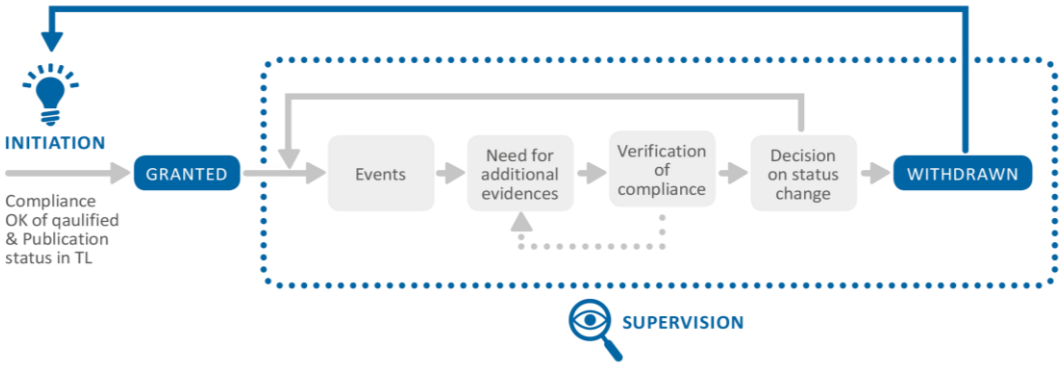

Figure 3 Supervision process flow

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.
  - Request and analysis of additional information which was necessary to verify compliance with the requirements laid down in eIDAS regulation.
  - Granting, a qualified status to the TSP and to the trust service(s) they provide, in case of positive verification.
- Publication of the qualified status in the national trusted list.

Once a qualified status is granted, the **supervision process flow** can be split into the following steps of related supervisory activities, as detailed in Figure 4, for each QTS at the level of granularity addressed in the national trusted list:

- The detection or notification of **events**: Those events will actually condition the next steps in the supervision process; each of those events may lead the competent SB to withdraw the qualified status of the corresponding QTSP/QTS:
  - 2-yearly anniversary from initial qualified status grant.
  - 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 **need for additional evidence**: This can consist in:
    - The SB requesting additional information or evidence from the QTSP.
    - The SB conducting an ad hoc audit.
    - The SB requesting a CAR from an accredited CAB.
- The **verification of compliance**: based on the event(s) data and the potential additional evidence, the SB will conduct a verification of the compliance of the concerned QTSP and its related QTSs. During that step, the SB may also face the need for additional evidence.
- The **decision on status change**: based on the results of the compliance verification, the SB may decide to keep the qualified status unchanged (granted) or to withdraw the previously granted qualified status. Once the qualified status has been withdrawn from a QTS and hence from its QTSP for the provision of that QTS, the corresponding TSP and trust service are "sent back" to the initiation process if the TSP wishes to be granted again a qualified status for that specific trust service.

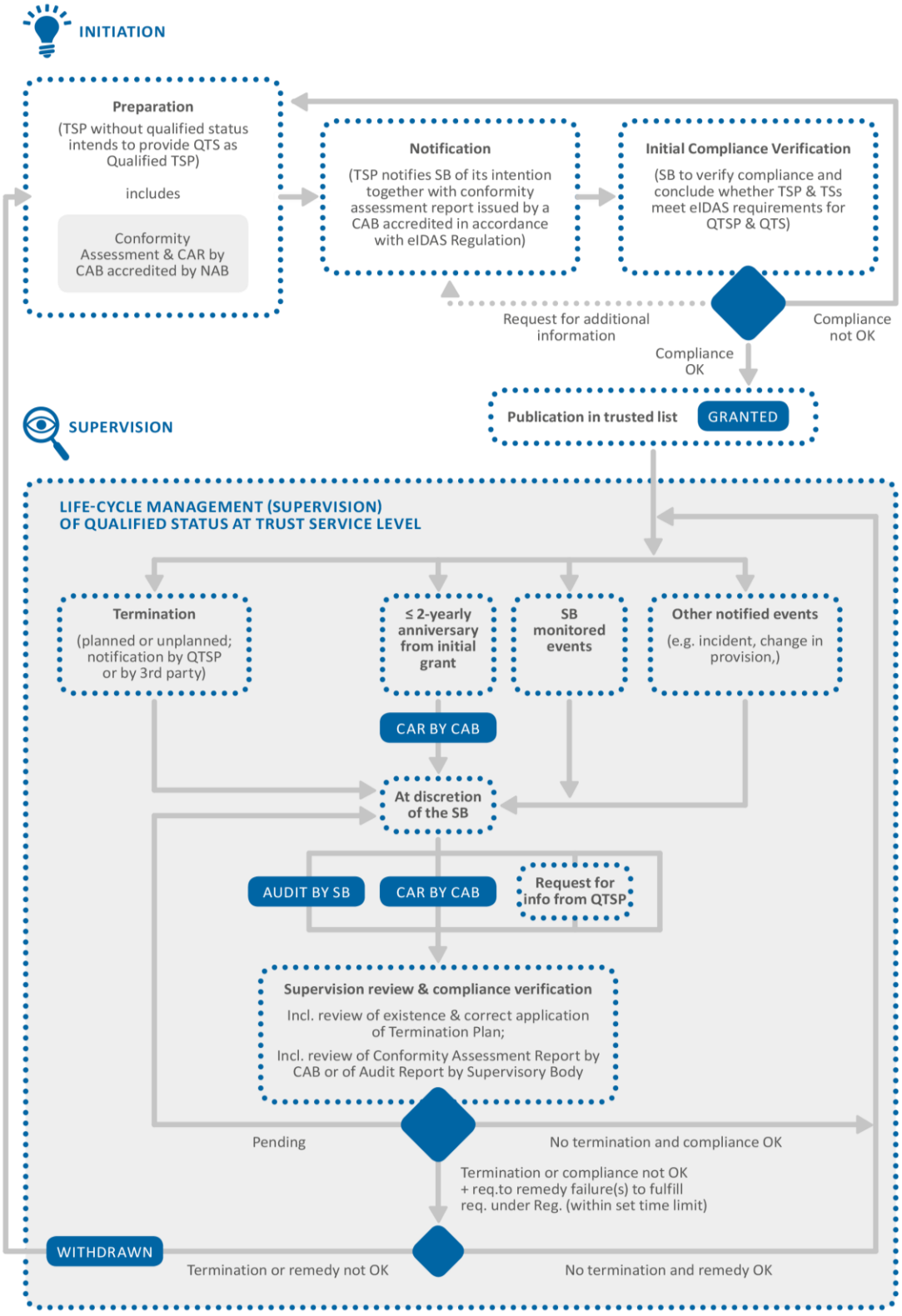

Figure 4 Overview of the QTSP/QTS initiation and life cycle management of the related qualified status at the trust service level and the related supervision activities. (Source IAS² - updated)

4.2.1 Documented policies, processes and procedures

With regards to the supervision activities in the context of the life cycle management of the qualified status of a QTSP/QTS, it is highly recommended, if not crucial, for SBs to establish, document and maintain policies, processes and procedures for the realisation of the supervisory activities foreseen in the eIDAS Regulation.

4.2.2 Due date file

With regards to the supervision activities in the context of the life cycle management of the qualified status of a QTSP/QTS, it is highly recommended, if not crucial, for SBs to continuously manage and update a consolidated deadline schedule and supervisory activities planner (hereafter referred to as the "due date file" or DDF).

This DDF should be designed to provide a complete overview of all the deadlines related to each and every QTS being granted a qualified status for each of the QTSP providing those QTSs. Those deadlines will relate to the planned supervisory steps, events and tasks regarding the supervised QTSs. The DDF should also allow for setting alarms sufficiently before the occurrence of those deadlines and for those alarms to be communicated to people in charge.

> Note: This is also a valid recommendation for QTSPs to maintain such a DDF at its level for each of the QTS that it provides and that are supervised by the competent SB.

SBs may consider sending reminders to QTSPs with regards to deadlines allocated to them, at least with regards to the most important ones (e.g. the due date for notification of a 2-yearly CAR).

SBs should also foresee, either under the (administrative) powers they have been given by the EU MS having designated them and/or in accordance with national laws, the various consequences for QTSPs failing to meet the supervision deadlines allocated to them.

SBs are also recommended to include in the DDF the deadlines related to the management of the national trusted lists for which they are competent, in collaboration with the designated bodies in charge of those trusted lists when they are different from the SBs. Relevant deadlines include, e.g., the expiration of the trusted list scheme operator (TLSO) certificates[27], the latest date and time before which the trusted list must be re-issued when no updated lists has been issued before that date.

4.3 Events

The events that will trigger specific supervisory activities with regards to the QTSP/QTS supervised by a SB can arbitrarily be grouped into five categories:

1. **Regular (2-yearly) audits**: From the date of the qualified status grant, QTSPs shall be audited at their own expense at least every 24 months by an accredited CAB. The purpose of the audit shall be to confirm that the QTSP/QTS fulfil the requirements laid down in the eIDAS Regulation. The QTSPs shall submit the resulting CAR to the competent SB within the period of three working days after receiving it. On reception of the 2-yearly CAR, the SB shall proceed to the verification of the eligibility of the

[27] Those are the certificates used to validate the signature created on the national trusted lists, as they are authenticated by the European Commission compiled list of pointers to the EU MS national trusted lists (see OJ C 233, 28.6.2016, p. 1–5).

CAR[28], assess the need for additional evidence (see section 4.4), proceed to the verification of the compliance of the concerned QTSP/QTS with the eIDAS Regulation (see section 4.5) and finally decide on maintaining or withdrawing the related qualified status (see section 4.6).

2. **Events monitored and detected by the SB**: contrary to the categories of events where the SB's role is passive, the SB should also actively monitor QTSPs/QTSs for which it is competent, to a reasonable extent and within the limits of the principles for good administration. Such an active monitoring may be driven by the results of previous verifications. It should also include proactive controls of QTSPs respecting:
   - the prohibition to provide QTS for which they have not been granted a qualified status as (not) indicated in the corresponding trusted list.

     Note: This includes for example the provision of claimed qualified certificates of a certain type while it has only been granted a qualified status for the issuance of qualified certificate for another type (e.g. the provision of QC for electronic seals or for website authentication while the issuing QTS is only allocated a qualified status for the provision of QC for electronic signatures). This also includes the provision of claimed EU qualified trust services while the provided services are not covered by the eIDAS Regulation (e.g. qualified certificates for encryption) or only covered by national laws (e.g. nationally approved archiving services).

   - the conditions and rules for use of the EU trust mark for qualified trust services.
   - the obligation to inform the SB of any change in the provision of its qualified trust services.
   - the applicable laws on consumer protection and misleading advertisement or cooperation with the relevant national bodies appointed to enforce these laws.
   - the provision of a CAR before 1 July 2017 if the QTSP was a CSP issuing qualified certificates to natural persons under Directive 1999/93/EC and if it migrated to being a QTSP issuing qualified certificates for electronic signatures under Art.51.3 of the eIDAS Regulation.

   On the detection of events whose importance would justify a further investigation, the SB shall assess the need for additional evidence (see section 4.4). Depending on those evidence, the SB may be required to proceed to the verification of the compliance of the concerned QTSP/QTS with the eIDAS Regulation and finally decide on maintaining or withdrawing the related qualified status.

   Depending on the number of QTSP/QTS that fall under its supervision, the SB may apply different types of strategies for such proactive controls, e.g. sampling techniques, regular checks of (changes on) QTSP/QTS publicly available commercials, websites, or policies and declaration of practices, mystery shopping, etc.

3. **Termination of one, more or all of the qualified trust services**: QTSPs must maintain, at all times, an up-to-date termination plan. That plan is to be agreed to by the SB and the compliance of the QTSP/QTS with it is regularly checked during the lifetime of the QTSP/QTS. That termination plan should cover, at least, expected and unexpected cessation of activities, the cessation of one, more or all the QTSs from a QTSP, the potential take-over of ceased activities by a third party or as at last resort

[28] See section 4.4 and the companion document "Guidelines on Initiation of Qualified Trust Services" for related recommendations.

by the SB[29], and the assurance of the preservation and the availability of the information referred to in Art.24.2.(h) of the eIDAS Regulation in accordance with the provisions laid down in that article.

QTSPs are required by the eIDAS Regulation (Art.24.2(a)) to inform the supervisory body of any intention to cease the provision of its QTSs.

Once being notified by the QTSP or by an authorised third party (e.g. in case of unexpected termination or bankruptcy), of the termination or the intention to cease the provision of its QTSs, partly or entirely, the SB shall verify the existence, the up-to-date character and the correct application of provisions laid down in the applicable termination plan including on how information is kept accessible in accordance with Art.24.2.(h) of the eIDAS Regulation. That verification may be subject to the assessment for the need of additional evidence (see section 4.4). Once the SB has the assurance that the concerned QTS(s) of the QTSP have been properly ceased or when the SB judges that those QTS(s) in cessation do not meet the eIDAS Regulation requirements anymore without any reasonable possibility to resolve the notified failures, then the SB shall withdraw their qualified status and notify the TLSO for updating the national trusted list accordingly.

4. **Other events notified by QTSPs**

   - **Results of surveillance audits not stemmed from the eIDAS Regulation**: While this is not a requirement stemming from the eIDAS Regulation, the conformity assessment scheme driving previous assessment of QTSP/QTS by an eIDAS accredited CAB may require more frequent surveillance audits from the CAB (e.g. annual). As an example, ETSI EN 319 403 requires:
     - The CAB to perform surveillance audits on at least a yearly basis besides the bi-annual full conformity assessment, and
     - The QTSP to report to the CAB changes in the provision of its qualified trust services that would affect its certification of conformity and the CAB to evaluate if a re-assessment is necessary.

     QTSPs may also wish to additionally meet the requirements of non-eIDAS application domain owners, e.g. CA/Browser Forum and Internet Brower software industry, which may similarly require yearly surveillance assessments.

     Hence it is recommended to the QTSP to synchronize in time, when feasible, the change notifications in order to undertake conduction of possible necessary re-assessment resulting from those changes at the time of the next regular surveillance or 2-yearly supervision audit.

   - **Changes in the provision of a QTS**: QTSPs are required by the eIDAS Regulation (Art.24.2(a)) to inform the supervisory body of any change in the provision of its QTSs. This obligation should not be limited to “significant” changes or to changes “the QTSP judges relevant for notifications”: it applies to “any” change in the provision of its QTSs. It is not up to the QTSP but to the SB to judge the relevance of any such change and of its consequences with regards to the retaining or withdrawal of the qualified status.

     Since it may be considered impossible to report literally any change in the provision of QTSs, mechanisms to classify such changes should be defined, ideally, by the SB and they should be

[29] See ENISA report “Guidelines on Termination of Qualified Trust Services” for further guidance.

harmonized among all SB's. Procedures should be established by the SBs and communicated to (Q)TSPs to deal with changes affecting the supervision and the grant of the qualified status. This includes notification of the change and determination of appropriate supervisory activities, including scope of ad hoc re-assessment, to assess that ongoing conformity is ensured. Notification and decision should be performed before implementation of the measures.

Examples of changes:

- Any change in the QTSs policies and related QTSP practices affecting the trust service must be (ideally proactively) notified to the SB.
- Any change in the initial notification information provided to the SB during the initiation of the QTS having resulted in the grant of a qualified status must be notified (e.g. change in the QTSP liability provisions, changes in the financial capacity or insurance coverage of the QTSP, changes in the termination plans).
- Major changes in the QTSP/QTS documentation.
- Any security relevant change.
- Adding (i.e. generating keys for) a new (technical) issuing CA under a (root) CA of which the corresponding public key is listed as a qualified trust service entry in the national trusted list is a change that must be notified to the SB.

- **Security and personal data breaches**: TSPs, including QTSPs, have an obligation under Art.19 of the eIDAS Regulation "to, 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".

  Art.19 of the eIDAS Regulation further requires that "where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay".

  The SB should establish and make available to TSPs, including QTSPs, the applicable procedures and means for reporting such breaches. In particular, the SB should provide guidance on identifying and analysing incidents and vulnerabilities, on determining how significant their impact in on the TSP, its services and personal data maintained therein, what data needs to be reported and the template of the report. The SB shall also provide simple facilities to the reporting TSP to ensure the confidentiality of the reported data. SBs should refer to the guidance and tools provided by ENISA as part of the Art.19 committee activities[30].

  Where the SB determines that disclosure of the breach of security or loss of integrity is in the public interest, it shall inform the public or require the trust service provider to do so.

  Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified SB shall inform the SBs in other EU MS concerned and ENISA (Art.19.2).

[30] See "Article 19 Incident Reporting", https://www.enisa.europa.eu/publications/article19-incident-reporting-framework".

5. **Other notified events**

   - **Complaints**: The SB should put in place complaints collection channels, complaint forms and procedures available to consumers and relying parties. On the reception of a complaint whose importance would justify further investigation, the SB shall assess the need for additional evidence (see section 3.4). Depending on those evidence, the SB may be required to proceed to the verification of the compliance of the concerned QTSP/QTS with the eIDAS Regulation and finally decide on maintaining or withdrawing the related qualified status.

   - **Request for cooperation from other SBs**: see section 5 of this document.

Each of those events may lead the SB to withdraw the qualified status of a QTSP/QTS.

Where the SB is notified or identifies events that may or will trigger specific supervisory activities with regards to the QTSP/QTS for which another EU MS SB is competent for its supervision, the SB should inform the concerned foreign SBs without delays.

4.4 Assessment of the need for additional evidence

When the SB is notified or when it identifies events that may or will trigger specific supervisory activities with regards to the QTSP/QTS it supervises, it should assess the need for additional information or evidence in order to facilitate the identification of the impact on the QTSP/QTS and the verification of their compliance with the eIDAS Regulation. This may include, at the discretion of the SB, requests for additional information from the concerned QTSP, the conduction of ad hoc audits by its own services, or requests for the CAB to perform a conformity assessment of the concerned QTSP/QTS, at the expense of the TSP, to confirm that they fulfil the eIDAS Regulation requirements.

With regards to their activities, SBs should respect, should, among other things, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality (see Recital (43) of the eIDAS Regulation). Therefore, SBs should duly justify their decisions to require such additional information, an ad hoc audit or an ad hoc conformity assessment by an accredited CAB.

4.5 Supervision verification of compliance

Where events notified to the SB or identified by it require a verification of the compliance of the concerned QTSP/QTS it supervises, the SB shall proceed to such a verification on the basis of the notified and/or collected information.

Depending on the nature and the severity of the event and its impact on the QTSP/QTS and depending on the severity of the resulting non-conformities with the requirements of the eIDAS Regulation, the SB may either decide to withdraw the qualified status of the impacted QTSP/QTS without delay or to require the QTSP to remedy those non-conformities.

When the supervisory body requires a QTSP to remedy any failure to fulfil requirements under the eIDAS Regulation, that SB should notify a clear time limit before which the notified failures must be solved by the QTSP.

As stated previously, SBs should note that the requirements applicable to the QTSP/QTS, for a specific type of QTS and at the granularity level used in accordance with the national trusted list, are those requirements laid down in the eIDAS Regulation. It is not allowed to impose QTSPs/QTSs any specific way

to proceed to implement those requirements and in particular to impose compliance with any specific standard, even partially.

The following recommendations apply on the steps to be undertaken by the SB with regards to the "supervision verification" phase:

1. Where the verification is based on a CAR (either ad hoc or 2-yearly), verify the eligibility of the CAR. The verification of the eligibility of the CAR includes verifying that
   (a) The CAR has been issued by a CAB accredited in accordance with the eIDAS Regulation (see section 2.3 and in particular section 4.4 of the companion deliverable "Guidelines on Initiation of Qualified Trust Services" for guidance).
   (b) The CAR provides sufficient information to demonstrate that the assessed QTSP/QTS fulfil each of the applicable eIDAS requirements in case of a 2-yearly CAR or each of the applicable set of requirements identified by the SB in case of an ad hoc CAR requested by the SB.

   When this verification is not satisfactory, indicate the non-conformities to the QTSP as well as the deadline for correcting them.
2. Clearly identify the name of the assessed QTSP, and where applicable its registration number, as stated in the official records, its official postal address and its electronic address.
3. Clearly identify the qualified trust service(s) of the QTSP that is(are) concerned by the verification, and in case of availability of a CAR, for which that CAR 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 and the content of the national trusted list.

   Note: Where a CAR is submitted, it 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.

4. Verify that the QTSP/QTS comply with the requirements laid down in the eIDAS Regulation, taking into account, for each (potentially) qualified trust service identified in point (3):
   (a) the detailed description of the functional (e.g. PKI) architecture or hierarchy,
   (b) the provided documentation,
   (c) the provided CAR,
   (d) other relevant information when not part of the notified documentation, e.g. information about QTSP financial resources or insurance, certification of QSCD, test samples of all types of outputs of the QTS, an up-to-date termination plan, trust service practice statement of practices and policies, subscriber agreements.

   That verification is to be performed requirement per requirement for each of the applicable requirements with regards to the type of QTSP/QTS. For that purpose, the structure of those requirements provided in point (10) of section 4.5 of the companion document "Guidelines on Initiation of Qualified Trust Services" as a recommended structure of the CAR 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[31] is to be judged by the SB as a last resort[32].

[31] 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.
[32] In that, the decision of the SB may overrule the CAB certification decision or non-conformity decision reported in the CAR by the CAB.

5. In the absence of non-conformity, or when the relevance and the severity of the identified non-conformity(ies) lead the SB to conclude that the QTSP/QTS does comply with the requirements laid down in the eIDAS Regulation, then the SB shall inform the QTSP that it and the QTS it provides and concerned by the verification retain their qualified status.
6. Where the relevance and the severity of the identified non-conformity(ies) lead the SB to conclude that the QTSP/QTS does not comply with the requirements laid down in the eIDAS Regulation, then the SB shall inform the QTSP of those non-conformities and, where applicable, of the time limit by which the QTSP must solve them.
7. Where the relevance and the severity of the identified non-conformity(ies) lead the SB to conclude that the QTSP/QTS does not comply with the requirements laid down in the eIDAS Regulation or where the QTSP, required by the SB to remedy notified failures, does not act accordingly, and within a time limit set by the supervisory body, if applicable, the SB, taking in particular into account the extent, the duration and the consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides[33]. The SB shall inform the body referred to in Art.22.3 of the eIDAS Regulation without any delay (hereafter the trusted list scheme operator or TLSO) for the purposes of updating the trusted lists referred to in its Art.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)[34] with regards to date and time of the issuance of the trusted list and the date and time of the withdrawal of the qualified status of the concerned trust services and as this latter will appear in the trusted list. As the QTSPs shall stop providing the qualified trust service after the qualified status has been withdrawn in the corresponding national trusted list, and as trusted lists have a constitutive value also for the relying parties, the date of the withdrawal of the qualified status must be aligned with the date of publication of that trusted list. No back dating is allowed.
9. During the verification process, the SB may require additional information from the notifying TSP and, where applicable, from the CAB having issued the submitted CAR.
10. The verification process should be concluded within a reasonable time frame[35] meaning in particular that, when leading to withdraw the qualified status of a QTSP/QTS, the elapsed time between the notification/identification of the cause event and the effective publication of the withdrawal of the qualified status in the national trusted list should be reasonable and proportionate to the nature of the non-conformities and may consequently be required to be as short as possible. If the verification is not concluded within a reasonable time frame, the SB shall inform the QTSP specifying the reasons for the delay and the period within which the verification is to be concluded.

[33] Noting that a TSP cannot be qualified without providing a QTS (Art.3.20 of the eIDAS Regulation).

[34] "The *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 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*".

[35] The eIDAS Regulation does not impose any (maximum) delay. The principles of good administration nevertheless apply.

4.6 Decision on status change – Qualified status withdrawal

If a QTSP/QTS fails to meet the eIDAS requirements, and if it fails to remedy failures notified by the SB within a time limit set by the SB, if applicable, this latter, taking in particular into account the extent, the duration and the consequences of those failures, may withdraw the qualified status of that provider or of the affected service it provides.

Where withdrawal of the qualified status of a QTSP/QTS is decided by the SB, it shall inform the body competent for the national trusted list without any delay for the purposes of updating that list (see point (8) of the previous section).

The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.

5. SB cooperation with other EU MS SBs

5.1 Mutual assistance

Art.18.1 of the eIDAS Regulation requires SBs to "*cooperate with a view to exchanging good practice*", and in particular, without prejudice of Art.18.2 detailing conditions under which a SB may refuse, it requires SBs, *upon receipt of a justified request from another supervisory body, [to] provide that body with assistance so that the activities of supervisory bodies can be carried out in a consistent manner. Mutual assistance may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21*.

SBs should treat such justified and acceptable requests as part of the "other notified events" in the context of the supervision process flow described in the present document.

When facing cross-border aspects of supervised QTSPs/QTSs, SBs should make such requests for cooperation to the concerned other SBs. SBs should also exchange information on potential issues regarding QTSP/QTS supervised in an EU MS:

- Being a subsidiary of another (Q)TSP established in another EU MS, or
- Mutualising PKI factory facilities with another (Q)TSP or another legal entity established in another EU MS.
- Making use of local of service provision (e.g. registration authorities in the context of issuance of qualified certificates) established in other EU MSs.

5.2 Exchanging good practices

With regards to the mutual cooperation with a view to exchange good practice, there are several domains where the SBs (and respective EU MS) should collaborate, allowing for increasing the transparency and the sharing of information at least on the following topics:

- Actual practices, policies, and procedures related to the supervisory activities of each SB.
- Facilitate mutual assistance and practices between SB in the context of cross-border supervision activities.
- Provisions on trust services set in the eIDAS Regulation, their interpretation and implementation by each SB and corresponding EU MS.
- Establishment of convergent certification schemes for CABs to be accredited in accordance with the eIDAS Regulation and accredited CABs to assess QTSP/QTS for compliance with the eIDAS Regulation;
- Assessment of available standards for supporting such certification schemes.
- Provide input, timing and priority considerations to the EC with regards to potential/optional adoption of implementing or delegated acts foreseen by the chapter related to trust services set in the eIDAS Regulation.
- Dissemination of information regarding the CABs accredited in accordance with the eIDAS Regulation and the context of the conformity assessment report.
  SBs could leverage on existing formal or informal groups, institutions or initiatives (e.g. FESA, ENISA, CEF, EU MS eIDAS experts groups, EC's eIDAS Observatory[36]) in order to exchange good practice and facilitate mutual assistance.

[36] See https://ec.europa.eu/futurium/en/eidas-observatory.

6. Bibliography/References

6.1 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

6.2 Bibliography

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

6.3 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

Notice: All Annexes mentioned in this document, refer to the corresponding numbers of Annexes included in the document “Guidelines on Initiation of Qualified Trust Services”.

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-06-16-341-EN-N

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

ISBN: 978-92-9204-190-8
DOI: 10.2824/361221