enisa

THE EU CYBER SECURITY AGENCY

GUIDELINES ON TERMINATION OF QUALIFIED TRUST SERVICES

Technical guidelines on trust services

DECEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU 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 EU 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 contacting the authors please use trust@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

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

ISBN: 978-92-9204-244-8
DOI: 10.2824/421172

Table of Contents

Notice: The present document is not expected to provide any kind of obligation or mandatory "requirement" but should be understood as recommendations or guidelines.

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
EC	European Commission
EEA	European Economic Area
eID	electronic Identification
EN	European Standard
ETSI	European Telecommunications Standards Institute
ETSI TS	ETSI Technical Specifications
EU	European Union
GDPR	General Data Protection Regulation
IAS²	IAS² European Commission Study – SMART 2012/0001 (see bibliography)
ISO	International Organization for Standardization
MS	Member State
OID	Object Identifier
OJ	Official Journal (of the European Union)
PKI	Public Key Infrastructure
QERDS	Qualified Electronic Registered Delivery Service
QESeal	Qualified Electronic Seal
QESig	Qualified Electronic Signature
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
QTST	Qualified Time Stamp Token
QValQES	Qualified Validation service for Qualified Electronic Signatures/Seals
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. Guidelines on termination of qualified trust services provision

1.1 Introduction

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

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

To further enhance in particular the trust of small and medium-sized enterprises (SME) 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[2] scheme of qualified trust service providers (QTSP) and the qualified trust services (QTS) they provide (hereafter referred to as a QTSP/QTS) by the national competent supervisory body (SB) that supervises, ex ante and ex post, fulfilment of the QTSP/QTS requirements and obligations.

Before a TSP/TS is granted a qualified status (becoming a QTSP/QTS), it will be subject to a pre-authorisation process – the so called initiation process[3] in line with Art.21 of the eIDAS Regulation. QTSP may only begin to provide the QTS after the qualified status has been granted by the national SB and indicated in the national trusted list as referred to in Art.22 of the Regulation. From there, the supervision scheme covers the full life cycle of each QTS and each QTSP, from its genesis until its termination.

To ensure sustainability and durability of QTS, and proper termination and user's confidence in the continuity of QTS, QTSPs have to maintain an up-to-date termination plan, as referred to in Art.24.2(i) of the Regulation[4]. The elaborating of such a termination plan from/before the start of QTS provisioning is crucial to ensure minimizing the impacts of the disruption of the service to its subscribers and relying parties and ensure the sustainability, legal certainty and evidential value of QTS generated evidence (QTS outputs[5]) that were created before QTS termination became effective (making sure that e.g. a

[1] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[2] See ENISA report "Guidelines on Supervision of Qualified Trust Services", https://www.enisa.europa.eu/topics/trust-services/guidelines/.
[3] See ENISA "Guidelines on Initiation of Qualified Trust Services", https://www.enisa.europa.eu/topics/trust-services/guidelines/.
[4] See Annex A.
[5] The term "QTS output" is used in the present document to refer to qualified certificates (for electronic signature, for electronic seal and/or for webs site authentication), qualified time stamps, QERDS evidence, qualified preservation statements or evidence for a qualified electronic signature/seal, qualified validation statements or reports on the qualified validation of a qualified electronic signature/seal, or a group of them.

QESig/QESeal, a qualified time stamp, a QERDS evidence created before the termination of the corresponding QTS will not lose its trustworthiness or validity because of that termination and it should still be possible to validate them afterwards)[6].

Termination plans have to be verified as compliant with the eIDAS Regulation by the SB upon initiation and regularly checked for compliance during the lifetime of the QTSP/QTS. Furthermore, Art.24.2(a) requires a QTSP to inform the SB of any change in the provision of its QTS and of an intention to cease those activities.

This document proposes guidelines to SB and (Q)TSP aimed at facilitating the implementation of the provisions related to trust services of the eIDAS Regulation in the area of termination of trust services. Termination of QTS is addressed here in a broad sense covering from partial to complete cessation of a QTS. Partial termination includes termination of one or more of (technical) service entries listed in the corresponding trusted list that are (collectively) used to indicate the grant of qualified status for the provision of a specific type of QTS.

The target audience of this document are (Q)TSP (including individuals, businesses and public administrations) who intend to start providing or are currently providing QTS and those EU MS SB designated to carry out supervisory activities under the eIDAS Regulation. Conformity assessment bodies (CAB) may also be interested in this document.

The objective of this document is to support QTSP making available QTS and SB in their respective tasks and duties regarding the termination and verification of compliance with the eIDAS Regulation as well as the management of qualified status through the publication of an updated national trusted list. These guidelines cover the procedures and formats for the termination and the supervision of the termination of a QTS. The guidelines shall enable SB to establish the rules, requirements and recommendations for a QTSP to manage the life cycle of the supervision of the QTS it provides, meeting the requirements of the eIDAS Regulation until and beyond the termination of those services.

The body of this document is purposefully kept short in terms of focusing on the effective high level guidelines and recommendations on termination of QTS provision as follows, while annexes are used to provide detailed guidance after brief description of the relevant eIDAS related requirements (section 1.2):

- General recommendations for (Q)TSP and SB (section 1.3)
- Recommendations on termination plan (section 1.4)
- Recommendations for SB (section 1.5)
- Recommendations for (Qualified)TSP (section 1.6).

[6] There might be circumstantiated cases where qualified certificates issued before the effective termination of the corresponding QTS (and QTSP) to be kept unrevoked and managed by a legal successor of the terminated QTSP. See section 1.2.5.1.

1.2 eIDAS provisions on termination of QTS

1.2.1 SB obligations

As part of the ex ante and ex post supervisory activities of QTSP established on their territory, Art.17.4.(i) of the eIDAS Regulation requires SB

- *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);*

Furthermore, without prejudice to the application of the principles of good administration, Art.20.2 allows SB, at any time, to audit or to request a CAB to perform a conformity assessment of the QTSP/QTS to confirm that they fulfil the requirements laid down in the Regulation, and in particular that they have, at any time, in line with Art.24.2.(i), an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the SB under Art.17.4.(i).

1.2.2 QTSP/QTS obligations

The legal obligations on QTSP related to the termination of QTSP/QTS are set out by points (i), (a) and (h) of Art.24.2 of the eIDAS Regulation.

As per Art.21.3, QTSP may begin to provide the QTS after the qualified status has been indicated in the trusted list of the MS in which it is established, hence after it has submitted a conformity assessment report from a CAB accredited in line with Art.3.18 of the eIDAS Regulation (Art.21.1) and after the competent SB, consequently to that submission, has verified that the notifying QTSP/QTS meets the requirements of the eIDAS Regulation and has granted qualified status to the applicant (Art.21.2).

As a consequence, the notifying TSP, without qualified status, intending to start providing QTS, is required to submit to the SB, a copy of its termination plan. The conformity of that termination plan shall be assessed and reported in the conformity assessment report -issued by a CAB-, which is submitted to the SB along with a notification of the TSP intention to start proving QTS.

1.2.3 CAB and CAR

Recommendations on the structure and 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 ENISA document “Guidelines on Initiation of Qualified Trust Services”.

1.2.4 Termination plan

As per Art.24.2.(i), a termination plan, aiming to ensure continuity of a QTS in accordance with provisions verified by the SB, needs to be available and up-to-date at any time/all times. Changes to the latest into force version, which has been verified by the SB, fall under the scope of the mandatory notification towards the SB as per Art.24.2.(a). Pursuant to Art.19.1, the termination plan needs to follow upon a risk assessment to ensure proper mitigation of risks.

Considering the granularity of the QTS related service entries as used in EU MS trusted lists, as defined in CID (EU) 2015/1505[7], a termination plan should cover the possible termination of each QTS related trusted

[7] The grant of a qualified status for a specific type of QTS can be indicated and managed in an EU MS trusted list through more than one service entry depending on the technical implementation of the provision of such a QTS by the QTSP. More than one trust anchor can be used corresponding to different PKI hierarchies, e.g. as the consequence of adoption of new technologies or for the purpose of serving different customer or business

list service entries and related technical components used to provide them. These trusted list service entries should be addressed both individually and collectively in the event of their individual termination, the termination of a group of them, or all of them.

The termination plan needs to include procedures and means allowing the (Q)TSP to meet Art.24.2.(h) of the eIDAS Regulation. This implies that it should still be possible to validate previous evidence created by the QTS or by means of QTS outputs. This may not require, except for qualified certificates (QC) specifically addressed by Art.24.2.(k), that the QTSP makes a copy of all such evidence from their creation but that the necessary elements for validating them would be made available (Art.24.2.(h): *all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service*). However, recording all data issued and received by the QTSP, for each type of QTS provided is recommended and may be proved helpful to achieve the objectives of Art.24.2.(h).

Regarding the period of time during which those data should be recorded and kept available, it needs to be *appropriate*, in particular with regards to the type of QTSP/QTS, and, when applicable, to the relevant legislation and/or rules related to the domain of application the QTSP/QTS aimed to support[8].

Considering requirements of Annex I.(b) & (g), Annex III.(b) & (g), Annex IV.(b) & (h), Art.33.1.(b), Art.42.1.(c), Art.44.(d), a QTSP may not transfer its QTS activities to another QTSP for the purpose of continuing the service under the name of the QTSP having terminated the QTS. As soon as the QTSP terminating the QTS ceases to be the provider, no other entity is entitled to create a new QTS output from the terminated QTS identifying the terminating QTSP as being the provider. Hence this will de facto require the cessation of the issuance of any new signed or sealed QTS output[9].

As a consequence, the termination plan may not include provisions for the creation of new QTS outputs that would indicate the QSTP having terminated the QTS as being the provider (QTSP) of such outputs (e.g. creation of new qualified certificates containing the identification data of the terminating provider as being the QTSP issuing that certificate).

The issuance of qualified certificates induces an additional layer in the sense that those certificates, and in particular the private key (signature/seal creation data) corresponding to the certified public key (signature/seal validation data) enables the signatory/seal creator to generate (qualified) electronic signatures/seals. Depending on the cessation scenarios, the possibility for such signatories/seal creators to continue to create signatures/seals may not be possible or authorised, or may lead to signatures no longer being recognised as qualified.

communities. More details on the granularity of the QTS related service entries as used in EU MS trusted lists can be found in the ENISA document "Guidelines on Initiation of Qualified Trust Services".

[8] As an example, compliance with EN 319 411-2 (clause 6.4.6.a) requires QTSP issuing qualified certificates to record and keep available Art.24.2.(h) data for a period of at least 7 years after any certificate based on these records ceases to be valid, i.e. from when it expires or is revoked. Application domains or sectoral regulations may require the period to be considered as being much longer than that.

[9] The term "QTS output" is used in the present document to refer to qualified certificates (for electronic signature, for electronic seal and/or for webs site authentication), qualified time stamps, QERDS evidence, qualified preservation statements or evidence for a qualified electronic signature/seal, qualified validation statements or reports on the qualified validation of a qualified electronic signature/seal, or a group of them.

1.2.5 Impact of termination on the qualified status

The impact of the termination of QTS on the qualified status of a QTSP/QTS will be influenced by the type of termination and the conditions under which it is executed.

Different types of termination can be distinguished, which are not necessarily exclusive:

(1) QTSP remains, or not, the final entity liable for QTS provision, with or without legal succession.
(2) Scheduled versus unscheduled termination.
(3) QTSP/QTS remains, or not, compliant with the requirements of the eIDAS Regulation.
(4) Partial versus global termination of the provision of a QTS.

The above list may not be complete in terms of different characteristics between different termination scenarios but these are the main cases on which the impact on the qualified status can be determined.

1.2.5.1 QTSP remaining or not the final entity liable for QTS provision

A. QTSP no longer liable entity for QTS provision without legal succession

One of the main principles in the context of QTSP/QTS termination is when the QTSP terminating the provision of a QTS (either partially[10] or globally[11]) will no longer be the final entity having legal liability and responsibility on the terminated QTS (or respectively on the terminated QTS service entries in the competent EU MS trusted list) and there is no transfer of obligation to a legal successor. Then, from the date and time at which this is effective, the following will apply:

1) The QTSP is not to be considered as a QTSP and not even a TSP anymore for the provision of that (those) service entry(ies) in the competent EU MS trusted list, and hence the qualified status of that (those) service entry(ies) in the competent EU MS trusted list should be withdrawn.

2) No new QTS output can be created:
   a) Under the name of the QTSP (i.e. signed or sealed with the name of the signatory or creator of the seal being the name of the (Q)TSP that terminated the service, or for QC, with the name of the issuer being still the name of the (Q)TSP that terminated the service for the issuance of the corresponding QC).
   b) By using the corresponding QTS service entry(ies), i.e. by using the private key(s) corresponding to the public key(s) identified in the QTS service entry(ies) of the competent EU MS trusted list.

   Note 1: Annex I.b&g, Annex III.b&g, Annex IV.b&h, Art.42.c, Art.44.1.d, and Art.33.1.b of the eIDAS Regulation require QTS outputs to identify the effective QTSP, as the signatory or seal creator when issuing such qualified outputs being respectively qualified certificates, qualified time stamps, QERDS evidence or (statements of) qualified validation of QESig/QESeal.

3) With regards to QTSP issuing qualified certificates, a QTSP that is about to terminate activities should revoke any still valid (un-revoked) qualified certificates in use.

[10] I.e. QTSP is terminating one QTS service entry, or more, representing an instance of a provided QTS, as listed in the competent EU MS trusted list.
[11] I.e. QTSP is terminating all QTS service entries representing one type of QTS, as listed in the EU MS competent trusted list.

Note 2: Once all unexpired and unrevoked qualified certificates have been revoked, the terminating QTSP issuing qualified certificates should issue a final CRL, and OCSP responses as appropriate. This final CRL and corresponding OCSP responses should be part of the Art.24.2.(h) referred data to be recorded and made available sufficiently long enough using procedures and technologies capable of extending the trustworthiness and unambiguity of the CRL and OCSP responses signatures/seals beyond the technological validity period, in the meaning of the *appropriate* period under Art.24.2.(h).

Note 3: Art.24.3 and Art.24.4 apply to a QTSP and not to the termination of the corresponding QTSP/QTS or even to the withdrawal of their qualified status. However, this is without prejudice to the obligations resulting from Art.24.2.(h) to provide certificate validity status information regarding each and every qualified certificate issued prior termination, as discussed in Note 2 above.

4) QTSP executes the procedures and means in order to meet Art.24.2.(h) of the eIDAS Regulation (see section 1.4, §4).

B. QTSP no longer liable entity for QTS provision with legal succession

When a QTSP is no longer the final entity bearing liability and having the responsibility to terminate the QTS since the obligations regarding the terminated QTS or respectively QTS service entry(ies) are transferred to another legal entity[12], the following provisions will apply:

(a) The legal successor may be the entity warranting the post-termination obligations (see section 1.2.2) of the terminating QTSP with regards to the terminated services (the legal successor entity does not need to be a TSP). When this is not the case, it needs to be ensured, prior to the termination by the terminating QTSP or as a last resource by the competent SB that an entity will take over these obligations.

(b) The legal successor may use the assets[13] of the trust services taken over to provide QTS, provided:
   a. The legal successor is a QTSP already qualified for the provision of the corresponding type of QTS[14].
   b. The legal successor notifies its competent SB of such a change in the provision of its QTS (Art.24.2.(a)). It is the responsibility of the SB to supervise the conformity of the QTSP and the QTS based on the requirements of the eIDAS Regulation. To this extent, the SB may at any time audit or request a CAB to perform a conformity assessment of the successor QTSP, at the expense of the QTSP (Art.20.2).
   c. The legal successor is generating new "Service digital identities" (i.e. new public/private key pairs when based on PKI technology) for inclusion of the QTS in the national trusted list once the qualified status is confirmed by the competent SB.

[12] The same may apply in case the QTS service entry(ies) is the result of a merger, acquisition or transfer of activities to another legal entity or when.
[13] Assets can include hardware and software allowing the provision of QTS, customer database and customer relationship management data and systems, suppliers' contracts, etc.
[14] When the legal successor is not a QTSP already qualified for the provision of the corresponding type of QTS, Art.21.1 initiation process must be undertaken prior to the provision of the corresponding type of QTS.

Note 4: Recertifying the corresponding public key(s) under the name of another QTSP, qualified for the provision of the same type of QTS should be discouraged mostly due to best practices[15] and security reasons. The same public key cannot appear twice in a trusted list for the same type of QTS as per CID (EU) 2015/1505.

However, recertification might be implemented together with the use of an Sie:TOB extension in case of a legal successor confirmed by a valid legal instrument and the alignment of the TSP trade names to reflect name matching. When the successor (Q)TSP is based in another EU MS than the one in which the terminating QTSP is established, it follows that supervision duties are reflected in the trusted list of the supervising MS. Nevertheless rekeying is strongly recommended when not required[16] for the purpose of interpreting the trusted lists contents for the same QTSP/QTS public key and minimising risks in line with Art.19.1 of the eIDAS Regulation.

(c) With regards to QTSP issuing qualified certificates, the revocation of all existing and unrevoked qualified certificates having been issued by the terminating QTSP before termination might not be necessarily carried out provided that:
   a. The legal successor of the QTS or respectively QTS service entry(ies) in the trusted list is a QTSP for the provision of the same type of QTS.
   b. The conditions of handling over the obligations[17] of the QTSP/QTS service(s) to the successor QTSP is legally (as per national laws) such that any reference to the former QTSP (i.e. name and registration number as in official records) are to be considered as identifying the successor QTSP (at least for the terminated QTSP/QTS service(s)). In this case a Sie:TOB extension should be used in order to reflect this in the trusted list corresponding service entry(ies) together with a reference to the national legislative instrument/court/statutory decision that make it effective[18].

As long as the eIDAS Regulation requirements are met, the status of those service entries taken over may be kept "granted" and service continuity is provided in line with recital 41 of the eIDAS Regulation. The SB should make sure that in the corresponding trusted list service entry(ies), all qualified certificates that do no longer meet Annex I criteria will be identified as "Not Qualified" (e.g. making use of appropriate extensions Sie:Q in the corresponding service entry(ies) or by withdrawing the qualified status for the corresponding service entry(ies)), as appropriate.

Replacing and revoking existing and unrevoked qualified certificates that have been issued by the terminating QTSP should however occur as soon as possible (in particular revocation of all QC no longer meeting Annex I, III or IV). Replacement means the provision of new qualified certificates issued by a QTS service operated by the successor QTSP under its own name.

---

[15] ETSI EN 319 401 requires that *before the (Q)TSP terminates its services all (Q)TSP private keys, including backup copies, are destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved* (clause 7.12).

[16] See above footnote.

[17] Such a transfer of obligations and of identification should be limited to the management of the QTS output created before the effective termination.

[18] Note that the sole use of Sie:TOB extension in the corresponding trusted list may not be sufficient to legalise such a transfer of identification as the eIDAS Regulation does not foresee such mechanisms. SB should make sure that an appropriate legal instrument is used to allow the continuation of the usage of the name of the terminating QTSP. A reference to that legal instrument should be included in the URI element of the Sie:TOB extension.

C. QTSP remains final entity liable for QTS provision

This case assumes the QTSP terminating or intending to terminate the provision of a QTS, either partially or globally, remains the final entity having legal liability and responsibility on the terminated QTS or respectively QTS service entry(ies).

That would allow, provided conformity will all applicable eIDAS requirements is ensured, the QTS to keep, until the effective termination, the qualified status being granted by the competent SB to those services under termination. It would also allow for QTS issuing QCs to keep the existing and unrevoked certificates unrevoked until subscribers receive new QCs or an alternative solution is provided. This situation does not prevent the QTSP to sub-contract external entities to meet its obligations on terminated services, prior and after their effective termination.

> Example 1: With regards to a CA/QC listed "Sdi" identified service, a QTSP may decide to stop issuing any new qualified certificate but between the date of stopping the issuance of any new qualified certificate and the effective termination of the QTS, it takes the necessary arrangements for its subscribers to receive new qualified certificate from another QTSP. As long as it is done for each and every subscriber, or after a certain time limit, it may revoke all unexpired and unrevoked qualified certificates and proceed to effective termination.

D. Normal decommissioning case

Normal decommissioning of QTS "Service digital identities" and/or specific service components, as normal operation, in the context of their life cycle may be ruled directly by the QTSP /QTS applicable policies and declarations of practices and may be excluded from the termination plan. Those decommissioning activities anyway fall under Art.24.2.(a) of the eIDAS Regulation and may be subject to the application of Art.20.2.

> Example 2: With regards to a CA/QC listed "Sdi" identified service, a QTSP may decide to stop issuing any new qualified certificate but to maintain all other component services until the revocation and/or expiration of all previously issued qualified certificates and of the issuing CA(s) and intermediate CA(s) in the PKI hierarchy leading to the listed CA/QC "Sdi".

In the above two latter cases (QTSP remaining the liable entity and normal decommissioning) when the termination is completed, the qualified status of the corresponding QTS service entry(ies) in the trusted list should be withdrawn.

1.2.5.2 Scheduled versus unscheduled termination

Unscheduled (or unplanned) termination of QTS and potentially of the entire QTSP activities can result from different causes, e.g. disaster or security breach from which only incomplete or unsatisfactory recovery could be reached, bankruptcy, court orders, and any other unexpected reason forcing the QTSP to undertake such a termination. In the context of an unplanned termination, the termination plan established for a planned termination should be followed as far as it is possible.

Nevertheless, the termination plan should be designed in such a way to circumvent and anticipate potential significant differences and difficulties to a scheduled termination, e.g. shorter time to update and actualise the termination plan, shorter or no "in advance" notification possibility towards the competent SB, the subscribers and the relying parties.

Prior arrangements should hence be established either with an external third party (e.g. notary) or with the competent SB to ensure proper execution of the termination plan's "unscheduled version" with the aim to meet requirements of the eIDAS Regulation.

1.2.5.3 Non compliance with eIDAS requirements

Whenever (during the life-cycle of a QTSP/QTS including termination) or as soon as it is clear for the SB that a QTSP/QTS does not meet the applicable eIDAS requirements any longer, its qualified status should be withdrawn for the QTS service entries in the national trusted list affected by such failure to meet the eIDAS requirements.

When not being the result of a termination process, the withdrawal of the qualified status of a QTSP/QTS should be considered as a forced termination of the QTSP/QTS for which the qualified status is withdrawn (Art.20.3).

Following the principles of good administration and Art.20.3, and in accordance with the severity of the identified non-conformities, prior to such a withdrawal, the competent SB should allow a reasonable time limit for the QTSP to remedy identified failure to fulfil requirements under the eIDAS Regulation.

This may however not always be possible or may require the time limit to be rather short, or inexistent, in particular in case of severe security incident or when the QTSP cannot be considered any longer as a TSP for the provision of the terminated trust service, e.g. when QTSP ceases to endorse final liability and responsibility on the terminated trust service.

1.2.5.4 Partial versus global termination of QTS

The principles described in the section 1.2.5.1 to 1.2.5.2 can be applied to each QTS entry in the national trusted list corresponding to each type of QTS subject to termination.

When not applied to all entries corresponding to a specific type of QTS, the termination can be referred to as a partial termination. When applied to all such entries, the termination can be referred to as a global termination.

1.3 General recommendations for (Q)TSP and SB

GEN.1 – Understanding the rules & obligations of (Q)TSP & SB with regards to QTS termination

Initiation

(a) (Q)TSP is required to establish a termination plan, compliant with the applicable eIDAS Regulation requirements, that will be submitted to the competent SB as part of the Art.21.1 initiation phase, i.e. as part of the notification of its intention to provide QTS (Art.21.1, Art.24.2.i & Art.24.2.h).
(b) The termination plan needs to be assessed by an eIDAS accredited CAB as part of the Art.21.1 initial conformity assessment of the (Q)TSP/(Q)TS against the eIDAS requirements (Art.21.1).
(c) The termination plan has to be verified as eIDAS-compliant by the competent SB as part of the Art.21.2 initial verification of compliance of the (Q)TSP/(Q)TS against the eIDAS requirements (Art.17.4.i, Art.21.1, Art.24.2.i).
(d) The design of the termination plan and its potential application may influence the implementation of other requirements of QTSP, regarding the QTS termination, including:
    (i) staff/subcontractors expertise, reliability, experience, and qualifications (Art.24.2.b)
    (ii) staff/subcontractors training (Art.24.2.b)
    (iii) sufficient financial resources and/or appropriate liability insurance (Art.24.2.c)
    (iv) user terms and conditions (Art.24.2.d)
    (v) use of trustworthy systems (Art.24.2.e & Art.24.2.f)
    (vi) use of best practices (Art.19.1)
    (vii) risk analysis and appropriate mitigation measures (Art.19.1, Art.24.2.g)
    (viii) lawful processing of personal data in accordance with Directive 95/46/EC (Art.24.2.j) and with the General Data Protection Regulation (GDPR) (EU) 2016/679, starting from May 2018.

Supervision

(a) Once granted qualified status for the provision of QTS, QTSP is required, to have and to maintain an up-to-date termination plan (Art.24.2.i).
(b) SB may at any time verify the existence and compliance of the termination plan (Art.20.2, Art.24.2i).

Termination

(a) QTSP has to notify the competent SB of any change in the provision of its QTS and the intention to cease those activities (Art.24.2.a), irrespectively of whether such cessation concerns part of the service or the entire regulated activity.
(b) QTSP should have appropriate procedures and processes to implement notifications referred to in point (a) above.
(c) Upon notification, SB will verify that termination plans are in place in case where the QTSP ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2) (Art.17.4.i).

GEN.2 – Interactions between (Q)TSP & SB

In order to allow for the efficient initiation and supervision process, as well as the efficient termination process, preliminary interactions between QTSP and the competent SBs are encouraged with a view to facilitating the due diligence leading to the provisioning and termination of QTS.

GEN.3 – Participation to ad hoc fora

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

1.4 Recommendations on Termination Plan

TP.1 – Scope and principles

The QTS termination plan should:

(a) Specify the procedures and arrangements for the termination of one, more or all QTS provided by a QTSP, or one, more or all components thereof used to provide its QTS.
(b) Address point (a) above to specify the level of granularity of the related service entries as listed in the corresponding national trusted list and the impact of such termination on those trusted list entries.
(c) Address point (a) above to ensure that,
    (i) after effective QTS termination, no QTS output can be created any longer by using the QTSP/QTS related signature/seal creation data previously used to create such outputs.
    (ii) before effective QTS termination, with regards to issuance of qualified certificates, the existing and unrevoked qualified certificates having been issued by the terminating QTSP are revoked, unless the conditions of handling over the obligations of the corresponding terminated QTS to a successor QTSP are met to ensure those qualified certificates and their management continue to meet eIDAS Regulation requirements, including Annex I, III, or IV (see Annex D, specific case).
(d) Cover especially the procedures and arrangements for the availability of its records for a determined duration, including all relevant information concerning data issued and received by the QTSP, in particular, for the purpose of providing evidence in legal proceedings, for GDPR legal compliances (audit on data collection and treatment) and for the purpose of ensuring continuity of QTS, in particular QTSP signature/seal validation data (e.g. signature/seal validation certificates) and continued maintenance of information required to verify the correctness of previously created QTS outputs.
(e) With regards to (d), QTSP should cooperate with the competent SB when it comes to identifying those records, their archival form and the way to ensure their future preservation and readability;
(f) Cover both voluntary and involuntary termination.
(g) Explicitly address identified scenarios for QTS termination (see TP.2 below).
(h) Include measures to ensure that the interests of the subscribers are safeguarded upon termination, including continued maintenance of information required to verify the correctness of previously created QTS outputs to which they had subscribed, and making arrangements with another QTSP so as they will receive new QTS in a less disrupting way (e.g. before revocation of previously issued QC).
(i) Address provision of notice to related parties
    (i) Potentially affected by the termination (i.e. “preventive” information as part of the QTS terms and conditions).
    (ii) Effectively affected by the termination (i.e. information resulting from the decision to execute or the execution of termination activities).

TP.2 – QTS termination scenarios

Recommendations on the following QTS termination scenarios to be considered by the QTS termination plan and their execution can be found in section 1.2.5 and in Annex D:

(a) [Scheduled] End of life cycle or decommissioning of the technical instance of a QTS corresponding to one or more service entries in a trusted list (e.g. private key usage period of CA/QC “Sdi” coming to an end, near future expiration of TSA/QTST TSU certificate).

(b) [Scheduled] Anticipated termination of QTS provisions; for example, for business reasons no new QC, QTST, QERDS evidence will be generated or provided to subscribers but all other component services are maintained:
    (i) By QTSP itself
    (ii) By a third party, or
    (iii) By SB in absence of third party or third party failure.
(c) [Scheduled] Takeover, merging or acquisition of QTS activities by another legal entity.
(d) [Unscheduled] Cessation due to a disaster or significant reason from which no satisfactory recovery is possible.
(e) [Unscheduled] Cessation due to a bankruptcy.
(f) [Scheduled]/[Unscheduled] Termination resulting from qualified status withdrawal.
(g) Etc.

TP.3 – Table of contents

Recommendations on the structure and content of the termination plan can be found in Annex C.

TP.4 – QTS termination plan associated documentation

The documentation associated with a QTS termination plan should include the following:

(a) Formal termination procedures.
(b) Formal termination procedures internal assessment (including regular internal assessment of the practical feasibility of the implementation of the termination plan).
(c) Formal termination procedures training.
(d) Formal termination procedures internal assessment reports.
(e) Formal termination procedures auditing reports.
(f) Formal termination (contractual) arrangements with 3rd parties (incl. subcontractors, taking over parties, SB).
(g) QTS terms and conditions, practices and policy documents.
(h) Up-to-date documentations for GDPR compliancy:
    (i) Treatment registers and data (and metadata) mapping
    (ii) Privacy impact assessments
    (iii) Documents (e.g. binding corporate rules) for peculiar cases of transfer outside Europe.

1.5 Recommendations for SB

SB.1 – QTS termination plan supervision

(a) Set-up specific review procedures and controls for verifying conformity and suitability of submitted QTS termination plan, following the above listed **GEN** and **TP** recommendations.
(b) Pursuant to point (a) above, recommend (Q)TSP to follow the structure and content of the termination plan that can be found in Annex C.
(c) Pursuant to point (a) above, use the termination plan structure and content in Annex C as a set of evaluation criteria or as a benchmark when assessing the termination plan of a (Q)TSP.
(d) Set-up controls and procedures to verify the availability from the QTSP side of a high level QTS termination plan and up-to-date policies, practices, procedures, process, 3rd party arrangements and other QTS termination plan associated documentation.
(e) Regularly verify the existence, compliance and appropriateness of the up-to-date QTS termination plan(s).
(f) Regularly verify QTS termination plan(s), at least every 2 years as part of the 2-yearly audit foreseen in Art.20.1, including verifying (Q)TSP internal assessments and CAB reports on QTS termination plan(s).

SB.2 – Procedures and means for reporting by QTSP of their intention to cease QTS

(a) Establish and make available to QTSP procedures and means to report their intention to cease QTS(s).
(b) Establish quality controls of such reporting procedures and means, and review them accordingly.

SB.3 – Confidentiality between SB and notifying (Q)TSP

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

(a) The verification and supervision of the execution of a QTS termination plan should always be undertaken taking into account the possibility that the qualified status of the terminated QTS may change in accordance with CID (EU) 2015/1505.
(b) In particular the SB and the TLSO shall respect the timing constraints clarified by CID (EU) 2015/1505 (enforcing clause 5.5.5 of ETSI TS 119 612 v2.1.1)[19] making sure that the date of the grant of the qualified status (indicated in the corresponding national trusted list), the date of signing of the trusted list and the effective date of publication of that trusted list are all aligned to the same date and that no back dating is allowed.

[19] ETSI TS 119 612 V2.1.1 (2015-07): Electronic Signatures and Infrastructures (ESI); Trusted Lists.

SB.5 – Cooperation with other EU MS SBs under Art.18 of the eIDAS Regulation

Cooperation under Art.18 between EU MS SBs is strongly recommended with regards to QTS termination plan verification to ensure equal treatment of QTS or QTSP termination and exchange of best practices. See Annex B for further guidance.

SB.6 – Good administration principles

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

SB.7 – Legislative instruments

Set up of appropriate legislative instruments ensuring proper execution of a QTSP/QTS termination plan, aiming proper implementation of Art.24.2.h, in particular in case of unscheduled termination such as bankruptcy.

1.6 Recommendations for (Q)TSP

TSP.1 – QTS termination plan establishment and management

(a) Establish QTS termination plans following the above listed **GEN** and **TP** recommendations.
(b) Set-up controls and procedures to ensure the availability of up-to-date policies, practices, procedures, process, 3rd party arrangements and other QTS termination plan associated documentation.
(c) Regularly review, update QTS termination plan(s) and assess them regularly.

TSP.2 – Properly communicate on the existence and updates of QTS termination plan(s)

(a) Without prejudice of notification obligations towards competent SB (Art.24.2.a) and of notification of impacted parties once activating a termination plan, QTSP should publicly communicate (e.g. through the update of CP/CPS, terms and conditions) on the existence and updates of QTS termination plan(s) towards customers, relying parties, relevant authorities and entities with which the QTSP has agreements regarding the QTS it provides.
(b) QTSP should include in their communication to subscribers (e.g. as part of the termination notification and as part of the CP/CPS, terms and conditions) information on:
    (i) The period of time during which QTSP will ensure Art.24.2.h referred data to be recorded and kept available and of the importance of the use by concerned parties of appropriate procedures and technologies capable of extending such a period when applicable, with regards to the data/records they are concerned with.
    (ii) The importance of the use of appropriate procedures and technologies capable of extending the trustworthiness of previously created QTS outputs and in particular on (qualified/advanced) electronic signatures/seals beyond the technological validity period. Those (advanced) electronic signatures/seals can be those placed on QTS outputs by QTSP or those created by subscribers on basis of their qualified certificate. Tutorials on how to efficiently use such procedures and technologies should be provided as well.
(c) QTSP intending to terminate QTS, partially or globally, should try to propose, sufficiently in advance, alternative similar solutions to their impacted subscribers. Such alternatives may be proposed by another QTSP with which terminating QTSP have made some appropriate agreements.

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

QTS termination should be designed to the level of granularity of the related service entries as listed in the corresponding national trusted list and to the impact of such termination on those trusted list entries.

TSP.4 – "Administrative" changes of QTSP natural or legal person

When considering and before implementing "administrative" changes to the natural or legal person acting as QTSP/QTS (e.g. change of name, merging, acquisition, bankruptcy, receivership, forced administration), the impacts of such changes should be carefully analysed with regards to the need for changing operations of the concerned QTS activities in order to comply with the provisions of the eIDAS Regulation (e.g. Annex I.b&g, Annex III.b&g, Annex IV.b&h, Art.42.c, Art.44.1.d, and Art.33.1.b), and/or for terminating them properly.

TSP.5 – Risk management

As part of Art.19.1 risk analysis, a termination specific risk analysis should be undertaken, documented and the associated mitigation measures should be documented and their implementation regularly controlled. This should include a personal data impact assessment and documentation of the associated mitigation measures.

TSP.6 – Financial Resources

Besides or as part of obligations from Art.24.2.(c) of the eIDAS Regulation, QTSP/QTS should maintain sufficient financial resources and/or obtain appropriate insurance to cover the costs required to properly execute the termination plan, particularly in case of unscheduled termination (e.g. in case of bankruptcy).

TSP.7 – Adoption of standards

When available, refer to best practices and standards on QTS termination (e.g. ETSI EN 319 401[20], clause 7.12; ETSI EN 319 411-2[21], clause 6.4.9; ETSI EN 319 421[22], clause 7.14).

[20] ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
[21] ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
[22] ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

2. References and bibliography

2.1 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

2.2 Bibliography

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

2.3 Relevant implementing acts

REF. ID	DESCRIPTION
(i)	Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services. OJ L 128, 23.5.2015, p. 13–15. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2015.128.01.0013.01.ENG
(ii)	Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 235, 9.9.2015, p. 26–36. http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015D1505
(iii)	Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 235, 9.9.2015, p. 37–41. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0006
(iv)	Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 109, 26.4.2016, p. 40–42. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D0650

Annex A: QTS termination as part of the supervisory activities

A.1 QTSP/QTS initiation and supervisory activities

The various steps foreseen in the eIDAS Regulation regarding the initiation of the QTSP and of the QTS it provides, and the related supervisory activities throughout the lifecycle of such services, from their genesis until their termination and even beyond that termination, can be depicted in the Figure 1 below.

The life cycle management of the ex ante and ex post supervision by competent SB to ensure that QTSP/QTS meet the requirements laid down in the Regulation can be split into the following phases:

- Initial compliance verification, including:
  - The analysis of the notification (procedure and format).
  - The analysis of the submitted conformity assessment report.
- Granting qualified status to the TSP and to the trust service(s) they provide.
- Regime management of the life cycle of the supervision of QTSP/QTS and the related supervisory activities, as they are conditioned by the following events, each of which having a possibility to lead to a change in the qualified status (withdrawn):
  - Regular audits
  - Ad-hoc audits and
  - Life-cycle events
    - Significant changes
    - Complaints
    - Security breach
    - Personal data breach
    - Service cessation / termination
    - Activities termination.

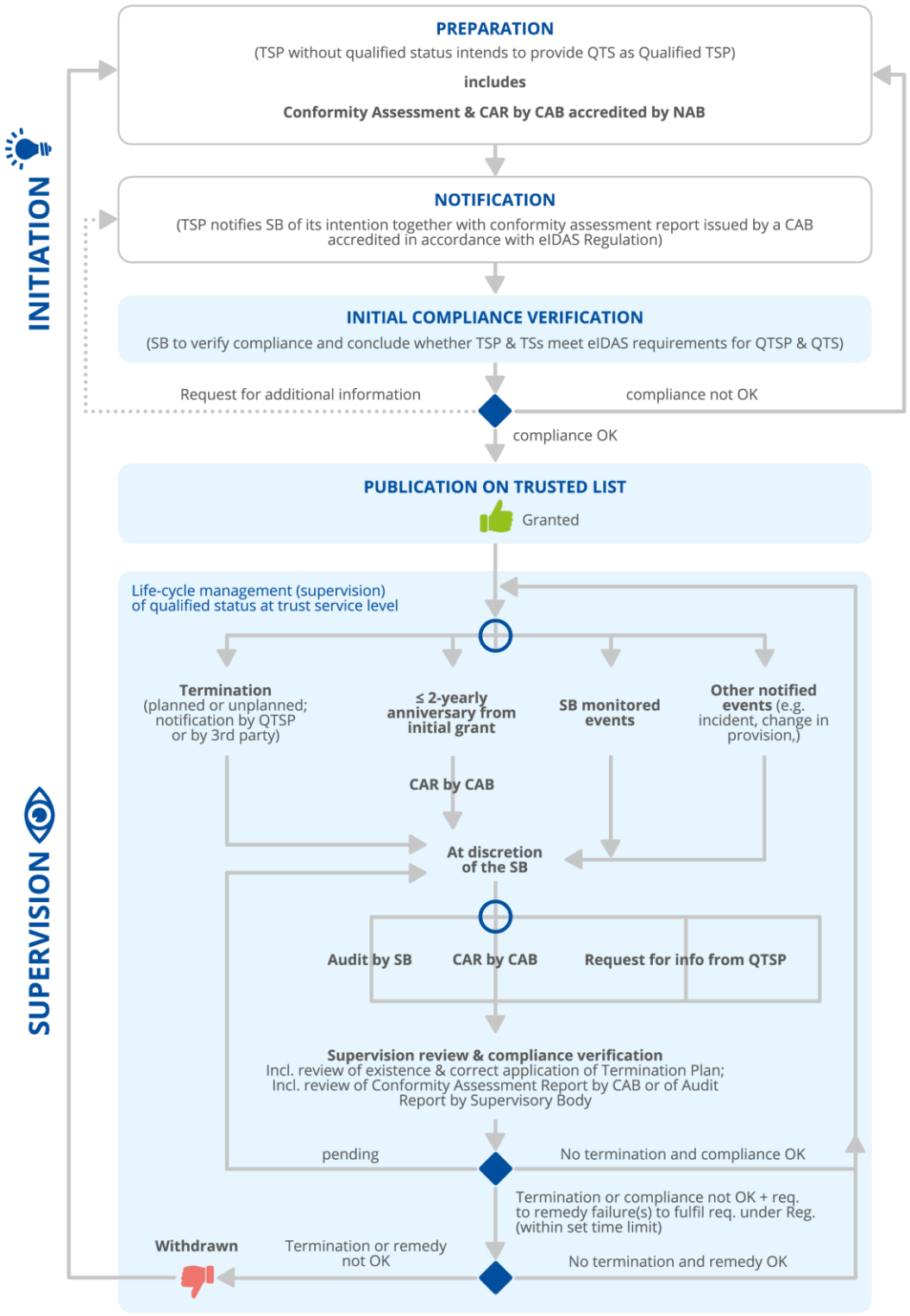

Figure 1: Overview of the QTSP/QTS initiation and life cycle management of the related qualified status at the trust service level and the related supervisory activities. (Source ENISA S-COD-16-T27)

A.2 QTSP/QTS termination of activities

To ensure sustainability and durability of QTS, as well as to ensure proper termination and user's confidence in their provision, QTSP are required to maintain an up-to-date termination plan. That plan needs to be verified as eIDAS-compliant by the SB as part of the initial grant of the qualified status and regularly checked for compliance during the life of the QTSP/QTS (Figure 2).

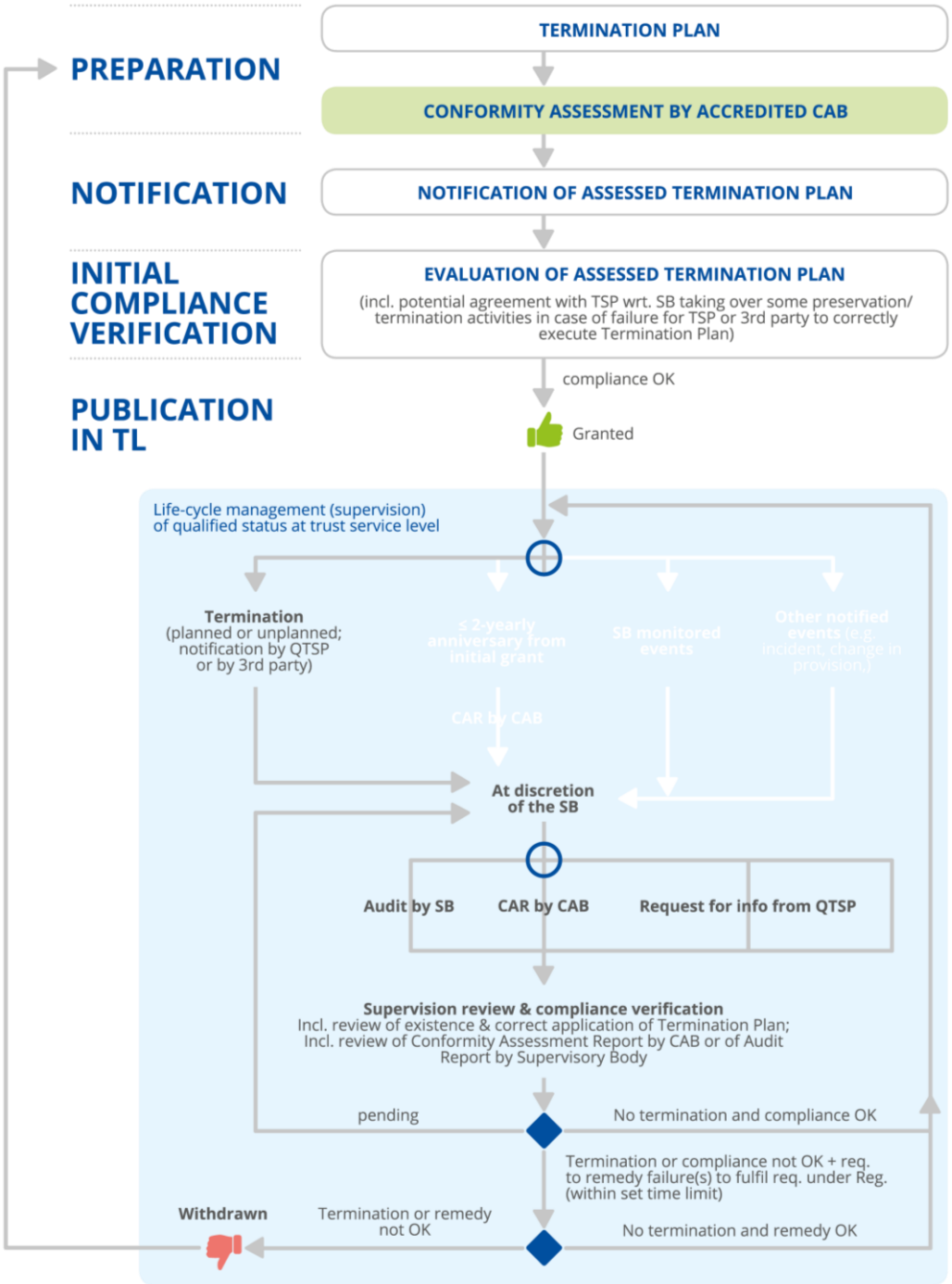

Figure 2: Detailed overview of the termination plan life cycle management and its potential execution

Having a more detailed view on the preparation, evaluation, supervisory activities and life cycle of a termination plan and its potential execution, Figure 2 illustrates the various steps to be taken into consideration. That termination plan should cover, at least, expected and unexpected cessation of activities, the cessation of one, more or all the QTS from a QTSP, the potential take-over of ceased activities by a third party or as at last resort by the SB, and the assurance of the preservation and 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.

QTSP are required by the eIDAS Regulation (Art.24.2(a)) to inform the SB of any intention to cease the provision of its QTS. Once being notified, by the QTSP or by any authorised third party (e.g. in case of unexpected termination or bankruptcy), of the termination or the intention to cease the provision of its QTS, partly or entirely, the SB will verify the existence, the up-to-date character and correct application of provisions laid down in the applicable termination plan including 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. 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 anymore the eIDAS Regulation requirements without reasonable possibility to resolve notified failures, then the SB will withdraw their qualified status and notify the TLSO for updating the national trusted list accordingly.

Various aspects should be addressed when considering the establishment and life cycle management of QTSP/QTS termination plan, its potential execution and the related supervisory activities:

- **Preparation**: It should include the writing and documentation of the termination plan itself but also the associated procedures, training and (internal/external) assessment plan for the personnel to correctly execute the plan when required.
  The plan should consider:
  - both scheduled and unscheduled termination of part of any QTS for which a qualified status is granted to a QTSP.
  - the termination of such a QTS as a whole.
  - the termination of more than one QTS.
  - up to the cessation of all QTS activities from a QTSP.

  It should cover all obligations as provisioned in the eIDAS regulation with regards to proper termination including the appropriate notification of the intention to cease such activities (Art.24.2.(a)) and the preservation and accessibility for an appropriate period of time, including after the activities of the QTSP have ceased, of all relevant information concerning data issued and received by the QTSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service (Art.24.2.(h)). These latter aspects may also trigger the need for ensuring, with respect to the type of QTS provided, the continuity in time of the validity of the evidence and legal effect associated to QTS outputs having been generated before their termination (e.g. termination of a QTS consisting in issuing QC for electronic signatures should ensure that QESig created by means of QCs before termination of the QTS can still be validated as QESig even after such a termination, QERDS delivery evidence should not be invalidated after termination of the related QTS by the QTSP, etc.).

  The risk of failure to properly execute the plan should be part of the risks analysed, assessed and mitigated with regards to termination activities and processes (Art.19.1).

  Guidelines for the establishment and (table of) content of a QTSP/QTS termination plan can be found in the present document.

- **Conformity assessment by eIDAS accredited CAB**: CAB should consider and use appropriate assessment criteria for the evaluation of the appropriateness of the termination plan established by a (Q)TSP, as part of the Art.21.1 initial audit and of the Art.20.1 regular audits.

- **Evaluation by a SB of a termination plan** as part of the information notified by a TSP under Art.21.1 initiation process and of the Art.20.1 notified audits: The present document provides guidance for SBs with regards to the evaluation of a notified and assessed termination plan established by a (Q)TSP. Specific attention should be paid by SB and EU MS on the potential need for taking over part or all termination activities in case of failure for the QTSP (or the expected taking over 3rd party) to correctly execute the termination plan. This may include recommendations on the set up of appropriate legislative instruments ensuring proper execution of a QTSP/QTS termination plan and in particular proper implementation of Art.24.2.(h) (e.g. in case of unscheduled termination such as bankruptcy).

- **Supervisory activities** related to termination plans in the context of QTSP/QTS life cycle supervision: SB should verify proper life cycle management by QTSP of a termination plan and ensure appropriate supervisory activities (including updating whenever a change in the provision of the QTS is scheduled or implemented and notified according to Art.24.2.(a), and internal/external assessment of the plan).

- **Effective termination and termination plan execution**: QTSP should properly implement/execute a termination plan. SB should monitor, evaluate and potentially take over execution of a termination plan, when required.

- **Impact on trusted lists** and related trusted list content management: SB should properly manage the impact on the content and management of trusted lists with regards to the execution of QTSP/QTS termination plans and the various circumstances underlying such terminations as they may be subject to different treatment with regards to the trusted lists content (e.g. use of “Service information extension” “Taken Over By” or not, trust service status change or not).

Annex B: SB cooperation with other EU MS SBs

B.1 Mutual assistance

Art.18.1 of the eIDAS Regulation requires SB 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 SB, *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*.

SB 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 QTSP/QTS, SB should make requests for cooperation to the other concerned SB. SB 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;
- mutualising PKI factory facilities with another (Q)TSP or another legal entity established in another EU MS;
- making use of local service provision (e.g. registration authorities in the context of issuance of qualified certificates) established in other EU MSs;

B.2 Exchanging good practices

With regards to the mutual cooperation with a view to exchange good practice, there are several domains where SB (and respective EU MS) should collaborate allowing to increase transparency and information sharing 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 conformity assessment (e.g. certification) schemes for CAB to be accredited in accordance with the eIDAS Regulation and accredited CAB to assess QTSP/QTS for compliance with the eIDAS Regulation;
- Assessment of available standards for supporting such conformity assessment 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;
- Rules applicable to CAB and CAR, and the related accreditation scheme in accordance with eIDAS;
- Dissemination of information regarding the CAB (validly) accredited in accordance with the eIDAS Regulation, the underlying accreditation schemes and their conformity assessment activities.

Annex C: Proposed table of contents for termination plan

C.1 Introduction

The existence of a termination plan compliant with the eIDAS Regulation requirements is de facto one of the prerequisite documentation for the (Q)TSP to be effectively granted a qualified status by the competent SB.

Since it is ultimately the competent SB that will take the decision to grant or not the qualified status to the assessed TSP/TS, Art.21.1 notification information (including the submitted conformity assessment report) should contain sufficient information to demonstrate, in detail to the SB, that the assessed TSP/TS fulfils the QTSP/QTS requirements laid down in the eIDAS Regulation. Regarding the termination plan, the eIDAS Regulation explicitly requires SB to verify, and hence agree, on the termination plan provisions with regards to the continuity of service and conformance with Art.24.2.h requirements.

It is in the interest of the SB to make recommendations on the structure and content of the termination plan so that it will be easier for the SB, in the boundaries of the principles of good administration and other similar applicable rules, to verify the suitability of submitted termination plans and the fulfilment of the applicable requirements.

SB are recommended to suggest or recommend (Q)TSP to follow the structure and content of the termination plan that can be found in Annex C.2. SB may use such a structure and content as a set of evaluation criteria or as a benchmark when assessing the termination plan of a (Q)TSP.

C.2 Table of contents

The specifications with regards to the structure and content of the termination plan referred to in Art.24.2.i of the eIDAS Regulation are recommended to include at least the following:

1. **Front page**
   - (i) **Document name & identification**: including versioning, date of entering into force, status and document classification.
   - (ii) **(Q)TSP identification**: Clearly identify the name of the (Q)TSP, and where applicable its registration number, as stated in the official records, its official postal address and its contact electronic address.
   - (iii) **Identification of concerned QTS.**
2. **Introduction**
   This clause identifies and introduces the set of provisions, and indicates the types of QTSP/QTS for which the termination plan is targeted.
   - **2.1. Overview**
     This clause provides a general overview of the termination plan and a synopsis of the QTSP/QTS to which termination provisions apply. Depending on the complexity and scope of the QTS provision, a diagrammatic representation may be useful here. All participants and QTS service components should be identified.
   - **2.2. Document name and identification rules**
     This clause provides any applicable names or other identifiers for the termination plan document and for relevant referenced documents, when applicable.
   - **2.3. QTS to which the termination plan applies**

This clause provides a detailed identification of the QTS to which termination provisions apply, in particular with regards to the corresponding national trusted list service entry(ies) and the associated "Service digital identity" elements (i.e. public keys when based on PKI). Depending on the complexity and scope of the QTS provision, a diagrammatic or table representation may be useful here.

2.4. Termination plan administration

This clause provides the name and mailing address of the organisation or authority that is responsible for the drafting, registering, maintaining, and updating of the termination plan. It also identifies the responsibilities and duties of that organisation or authority with regards to the QTSP/QTS termination, termination plan reviewing, internal/external auditing processes, and its execution.

This clause also includes the name, electronic mail address, telephone number, and fax number of a contact person, service or functional role.

2.5. Applicable national legislation and relevant provisions on QTSP/QTS termination

This clause provides references to the applicable national legislation and identifies the relevant national provisions on QTSP/QTS termination.

2.6. Definitions and abbreviations

This clause contains a list of definitions for defined terms used within the document, as well as a list of abbreviations used in the document and their meanings.

3. Termination plan provisions

3.1. Scheduled termination

This clause describes the provisions and actions to be undertaken:

- In the context of the scheduled termination of part or of whole of the QTS to which the termination plan applies; and/or
- In the context of the scheduled actions that could result in the partial or complete termination of the QTS to which the termination plan applies.

The arranged/contracted custodian(s), insurers or 3rd parties involved in assisting the implementation of the termination should be properly identified and their role and scope of assistance should be clearly described.

The relevant actions and the associated provisions should include:

- Termination plan update and the provisions on its notification to the competent SB.
- Identification of the operations to be ceased and the expected timing/scheduling.
- Identification of the expected impact on the relevant entries of the trusted list.
- Risk analysis update and updated mitigation measures.
- Financial resources and/or appropriate insurance to cover the costs required to properly execute the termination plan.
- Personal data impact assessment update and updated mitigation measures.
- Termination notifications
    - Identification of the entities to be notified of the termination (e.g. SB, subscribers, relying parties, other (Q)TSP with which the terminated service has trust relationships, QTSP staff and/or subcontractors).
    - For each notified entity or logical group of notified entities, specify the provisions on the termination notifications, the notification means and the expected timing/scheduling of those notifications.
    - Associated documentation.
    - Identification of the services whose termination is scheduled, the reason for such termination and the expected timing/scheduling.
    - Terms and conditions ruling the notified termination. This may include:

- Arrangement(s) applicable with another QTSP for the provision of future QTS of similar nature.
- Preservation of subscriber's related (personal) data.
- Preservation of operational data and other relevant data to sustain the trustworthiness of the QTS outputs and related evidence.
- With regards to qualified certificates, the conditions on continuation of use or their revocation for unexpired certificates.
- Foreseen compensations to subscribers, when applicable.

- Procedures for termination actions execution.
- Identification of the personnel (staff and/or subcontractors), the requested expertise and the training conditions.
- Transfer of recorded, auditing and archival records to the arranged/contracted custodian(s), and proper identification of custodian(s).

3.2. Unscheduled termination

This clause describes the provisions and actions to be undertaken:

- In the context of the unscheduled termination of part or of whole of the QTS to which the termination plan applies, and/or
- In the context of the unscheduled actions that could result in the partial or complete termination of the QTS to which the termination plan applies.

Unexpected or unscheduled termination of the QTSP/QTS may result from different causes such as severe incident or disaster from which incomplete or unsatisfactory recovery could be reached, bankruptcy, court orders, and any other unexpected reason forcing the QTSP/QTS to execute a termination.

This clause should address provisions and actions similar to those covered in clause 3.1 taking into account the unexpected and unscheduled nature of the causes for termination, and the potential limited time space within which those actions need to be undertaken.

The arranged/contracted custodian(s), insurers or 3rd parties involved in assisting the implementation of the unscheduled termination should be properly identified and their role and scope of assistance should be clearly described.

4. Compliance internal/external audit and other assessment

This clause addresses internal and external audit and other assessment, in particular:

- The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment.
- Frequency of compliance audit or other assessment.
- The identity and/or qualifications of the personnel performing the audit or other assessment.
- The relationship between the assessor and the QTSP whose termination plan is being audited, including the degree of independence of the assessor.
- Actions taken as a result of deficiencies found during the termination plan audit or other assessment.
- Internal/external person(s) entitled to be communicated the results of an assessment, and/or the actions taken as a consequence.

5. Other provisions

This clause provides any other applicable provisions not neatly fitting in any above clause.

Annex D: Guidance on termination scenarios

D.1 Takeover, merging or acquisition of QTS activities

Situation description

QTSP A, being established in country CCA, is providing QTS of a certain type. TSP B from country CCB is aiming to acquire QTS activities from QTSP A and use them to provide QTS in CCB, in CCA and in other countries.

Sub-cases:

(a) CCA = CCB
(b) TSP B is not a QTSP in CCB
(c) TSP B is a QTSP in CCB

Guidance principles

In the event TSP B takes over activities of QTSP A (a legal entity different from TSP B), in such a way that QTSP A is no longer the legal entity responsible for the provision of QTS, then from the effective date of such a takeover:

(i) No new QC may be issued under the name of QTSP A, at least with regards to the CCA trusted list CA/QC service entries and the type of QC concerned by such a QTS takeover (Annex I.b&g, Annex III.b&g, Annex IV.b&h).
(ii) No new qualified time stamp may be issued under the name of QTSP A (at least with regards to the CCA trusted list TSA/QTST service entries concerned by such a QTS takeover) (Art.42.c).
(iii) No new AdESig/AdESeal can be created under the name of QTSP A in the context of the provisioning of QERDS (Art.44.1.d), qualified validation of QESig/QESeal service entries concerned by such a QTS takeover (Art.33.1.b).

From the effective cessation of the QTS by QTSP A, SB may withdraw the qualified status of the CCA trusted list QTS service entries concerned by such a takeover. Furthermore, TSP B, when not having already been granted a qualified status for the type of QTS being taken over from QTSP A, may not provide any such QTS before being granted a qualified status from the competent SB of CCB following execution of Art.21.1 initiation process.

When having already been granted a qualified status for the type of QTS taken over from QTSP A, QTSP B is required to notify the competent SB of CCB of that change in its provisions in accordance with Art.24.2.a. CCB SB would then be required (Art.17) or at least entitled to assess and verify such changes and their compliance with the provisions of the eIDAS Regulation (Art.20.2). SB may request additional information from QTSP B and may conduct auditing activities or require a CAB having been accredited in line with Art.3.(18) of regulation (EU) 910/2014 to undertake specific assessment activities[23].

[23] Strictly speaking when QTSP B has already been granted a qualified status for that type of QTS, there is no need for a notification under Art.21.1. However, a notification under Art.24.2.a is required when the takeover of QTS by QTSP B implies a (significant) change in the provision of its qualified trust services. That notification under Art.24.2.a is not meant to be suspensive. Nevertheless, following such a notification and subsequent supervisory activities (e.g. verification, assessment) the competent SB, in line with Art.20.2, "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". This needs to be made under the principle of good administration.

The new (Q)TSP/QTS B "Sdi" resulting from the takeover would need to be listed in QTSP B section of CCB trusted list, even if the entire QTS infrastructures are kept being located and operated in CCA. Note that re-certification is not explicitly prohibited when CCA is different from CCB, as the rules requiring that an "Sdi" public key shall not be listed more than once for the same QTS type only covers the perimeter of a single trusted list (CID (EU) 2015/1505). Recertification might however be implemented and reflected even in a single trusted list together with the use of an Sie:TOB extension in case of a legal successor (confirmed by a valid legal instrument) and aligning the TSP trade names to reflect name matching. Nevertheless, rekeying is strongly recommended when not required (e.g. ETSI EN 319 401) for the purpose of interpreting the trusted lists contents for the same QTSP/QTS public key and minimising risks in line with Art.19.1 of the eIDAS Regulation. Art.17.1, Art.17.3 and CID (EU) 2015/1505 prevent in practice a TSP to be listed in different trusted lists from different EU MS.

Clause 5.5.9.3 of standard TS 119 612 2.1.1 does not contradict any provision of the eIDAS Regulation as it actually clarifies that Sie:TOB extension must be used in accordance with the applicable rules, in the present case being the ones from the Regulation. In such a context, the scope of the Sie:TOB extension is more to be used in the context of the cessation of a service (entry) and the taken over of the duties and obligations resulting from that takeover. This includes mainly the obligations regarding the continuity of the service to ensure the persistence and trustworthiness of the evidence created by the service before its termination.

Annex I.b&g, Annex III.b&g, Annex IV.b&h, Art.42.c, Art.44.1.d, and Art.33.1.b require QTS outputs to identify the effective QTSP, as the signatory or seal creator when issuing such qualified outputs being respectively qualified certificates, qualified time stamps, QERDS evidence or (statements of) qualified validation of QESig/QESeal.

SBs and Trusted Lists

The borderline between MSs with regards to the supervision of the two (Q)TSPs concerned by such a takeover is drawn taking into account the places of establishment of the (Q)TSPs. CCA will be responsible of the supervision of the proper termination of QTSP/QTS A and CCB will be responsible for supervising (Q)TSP B, wherever the respectively used infrastructures are physically located. However, when such infrastructures used by a QTSP for the provision of its QTS is partially or totally located in another country than the one in which it is established, a collaboration could be needed between the EU MSs involved (in line with Art.18). Decision to grant or withdraw a qualified status will however remain in hands of the competent SB.

With regards to CA/QC QTS, the new CA/QC certificates of the (Q)TSP B cannot be listed in the trusted list of the EU MS in which the QTSP A is/was established when this EU MS is not the one in which the (Q)TSP A is established. As per Art.17.1, the competent SB is expected to be in the EU MS in which the (Q)TSP is established, since it applies that each EU MS notifies one (or more) national body(ies) as SB. Delegation of duties to another SB from another EU MS as foreseen in Art.17.1 of the eIDAS Regulation is not supposed to be an "à la carte" delegation and in all cases should be the result of bilateral agreements between the concerned SB and EU MS.

When both QTSP A and QTSP B are established in the same EU MS, the new CA/QC certificates of the (Q)TSP B can only be based on new key pairs. Best practices, e.g. EN 319 401, require that *before the (Q)TSP terminates its services all (Q)TSP private keys, including backup copies, are destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved*.

Continuation of issuance of QTS outputs

Regarding the continuation of issuance of QTS outputs on the basis of technical instances corresponding to service entries (Sdi) associated to the QTSP A:

- End-entity QC is required, from the date of the takeover, to include the name of the QTSP B in such a way that that QTSP B is clearly and unambiguously identified as the legal (or natural) entity legally responsible for the provision of the associated QTS (Annex I.b/III.b/IV.b). Not changing the "O=" attribute in the Issuer DN would create confusion with regard to the actual entity having final legal responsibility on the corresponding QTS. Even if it would be technically possible to provide information on the name and identifier of the new (legal or natural) entity acting as QTSP, that information would likely not be machine processable and not conveyed in a standardised way. This would in any way create ambiguity and therefore non-compliant QC should be revoked.
- The QTSP A should not anymore be authorised to sign or seal under his name any QTS output from the date of its takeover by (Q)TSP B. Neither the QTSP B should be authorised to do so under the name of the QTSP A. This applies to issuance of any new QC after such takeover, the issuance of any new QTST, any new QERDS evidence, and any new QValQES report. Even signing OCSP response or CRLs under its name would be highly questionable.
- The same Sdi cannot be listed twice in the same TL for the same service type. Hence an Sdi cannot be moved from one QTSP to another in the same TL for the same QTS type even with a different certificate (recertification) identifying the new QTSP as the owner of the corresponding private key and hence as the signatory or seal creator.
- Listing the same Sdi a second time but in another EU MS TL for the same service type would in practice be possible but with new certificates identifying the QTSP B. However, this is strongly not recommended as previously indicated.

As a result, the qualified status of the QTSP A should be withdrawn with regards to the QTS having been taken over by QTSP B, when and since QTSP A is not any longer a QTPS for the provision of that type of QTS.

When the QTS consisted in the issuance of QC, this may have consequence for still valid (un-revoked) QC that will not be considered as qualified anymore (e.g. non-compliance with Annex I or issuing entity not a (Q)TSP any more) and hence not supporting anymore any QESig/QESeal or qualified website authentication.

Furthermore, before it terminates its CA/QC service(s) and before destroying its corresponding private keys, the QTSP A should revoke still valid (un-revoked) QC. They will anyway not meet any longer point (b) of Annex I, II or IV as the issuer is no longer a QTP issuing QC for that(those) service(s).

Specific case for not necessary qualified certificates revocation

With regards to QTSP issuing qualified certificates, the revocation, before effective termination of still valid (un-revoked) qualified certificates having been issued by the terminating QTSP A before termination, might not be necessary carried out that:

- The TSP B taking over the terminated QTS or respectively QTS service entry(ies) in the trusted list is a QTSP for the provision of the exact same type of QTS.
- The conditions of handling over the obligations[24] of the terminated QTSP/QTS service(s) to the QTSP B is legally (as per national laws) such that any reference to the QTSP A (i.e. name and registration number as in official records) are to be considered as identifying the QTSP B(at least for the terminated QTSP/QTS service(s)). In such a case a Sie:TOB extension should be used in order to reflect this in the trusted list corresponding service entry(ies) together with a reference to the national legislative instrument/court/statutory decision that make it effective.

[24] Such a transfer of obligations and of identification should be limited to the management of the QTS output created before the effective termination.

As long as the applicable eIDAS Regulation requirements are met, the status of those service entries taken over may be kept "granted". SB should make sure that in the corresponding trusted list service entry(ies), all qualified certificates that are no longer meeting Annex I will be identified as "Not Qualified" (e.g. making use of appropriate extensions Sie:Q in the corresponding service entry(ies) or by withdrawing the qualified status for the corresponding service entry(ies)).

Replacement and revocation of still valid (un-revoked) qualified certificates having been issued by the QTSP A should however occur as soon as possible (in particular revocation of all QC no longer meeting Annex I, III or IV). Replacement means the provision of new qualified certificates issued by QTS service operated by the QTSP B under its own name.

D.2 Merger by incorporation

Situation description

Merger by incorporation of one legal entity (QTSP) into the parent company ((Q)TSP), while before there were two distinct legal entities (different VAT and registration numbers).

Guidance principles

When the merged legal entity remains the entity having final legal liability and responsibility over the QTS it provides, such a merger should not be considered as a termination and Sie:TOB extension should not even be used.

When the merged legal entity does not remain the entity having final legal liability and responsibility over the QTS it provides or ceases to exist from a legal point of view, then principles described in section 1.2.5 should be applied to reflect such a case (including e.g. whether or not the incorporating entity intends to provide QTS or not, is already or not a QTSP for the provision of the corresponding QTS provided by the merged entity).

D.3 QTSP change of name

Situation description

The QTSP is changing only name but keeps other identifiers (e.g. exact same VAT and registration number).

Guidance principles

This should not be considered as a termination case per se but this will likely require the TSP to recertify or rekey its QTS service component used to sign or seal the QTS outputs. Specifically, when issuing qualified certificates, an update of the qualified certificate profiles may be necessary to continue to meet Annex I, III, or IV of the eIDAS Regulation.

Principles described in section 1.2.5 should be followed considering the case for which the QTSP remains to be the final entity liable for the provision of the QTS and considering normal decommissioning of QTS entries resulting from a change of name and its consequences (as described in the above paragraph).

D.4 Failure to meet eIDAS Regulation and withdrawal of qualified status

Situation description

This case applies when the QTSP fails to meet the eIDAS Regulation requirements, does not succeed to remedy any failure to fulfil eIDAS requirements and does not act accordingly, and if applicable within a time limit set by the SB. As a consequence, the SB, 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. When not already being the result of a termination process, the withdrawal of the qualified status of a QTSP/QTS should be considered as a forced termination of the QTSP/QTS for which the qualified status is withdrawn (Art.20.3).

A specific sub-case of such a general case is related to the transitional measures laid on in Art.51.3 and Art.51.4 of the eIDAS Regulation requiring certification-service-provider issuing qualified certificates under Directive 1999/93/EC and considered as qualified on entry into force of the Regulation for trust services to submit a conformity assessment report to the SB as soon as possible but not later than 1 July 2017. If a certification-service-provider issuing qualified certificates under Directive 1999/93/EC does not submit a conformity assessment report to the SB within the time limit referred to in paragraph 3, that certification-service-provider shall not be considered as QTSP under this Regulation from 2 July 2017.

Guidance principles

When as a result of such a withdrawal, the QTSP/QTS is terminated or the QTSP decides to terminate the corresponding non-compliant QTS, the principles described in section 1.2.5 should be applied to the specific type and case of QTS termination, partial or global, considering whether the QTSP remains or not the final entity liable for QTS provision, whether the termination is scheduled or unscheduled, and whether the QTSP/QTS remains or not compliant with the requirements of the eIDAS Regulation.

QTSP having benefited from Art.51 transitional measures must have a termination plan since 01 July 2017 and it is the responsibility of the competent SB to supervise the existence and correct execution of such a plan (Art.17.4.i, Art.24.2.i).

D.5 Business driven decisions

Situation description

Several business driven decisions may trigger cessation of activities related to the provision of QTS.

- When a CA/QC listed “Sdi” identified service is used to issue several types of qualified certificates, the QTSP may decide:
  - to cease the provision of qualified certificates of certain type(s) only and keep issuing the provision of other type(s) of qualified certificates, or
  - to cease the provision of all types of qualified certificates.
- When a CA/QC listed “Sdi” identified service is used to issue qualified and non-qualified certificates, the QTSP may decide:
  - to cease the provision of qualified certificates of certain type(s) only and keep issuing the provision of other type(s) of qualified certificates.
  - to cease the provision of all types of qualified certificates but keep issuing non-qualified certificates.
  - to cease the provision of all types of qualified and non-qualified certificates.

The above cessation examples may also be partial rather than global when considering one type of QTS.

Guidance principles

The principles described in section 1.2.5 should be applied to the specific type and case of QTS termination, partial or global, considering whether the QTSP remains or not the final entity liable for QTS provision, whether the termination is scheduled or unscheduled, and whether the QTSP/QTS remains or not compliant with the requirements of the eIDAS Regulation.

TP-06-17-471-EN-N

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 Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU 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 EU 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.

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 Str
151 24 Marousi, Attiki, Greece

enisa.europa.eu

ISBN 978-92-9204-244-8
doi: 10.2824/421172