EY eIDAS Certification Scheme (accredited scope)

for qualified trust service providers (QTSP) and the qualified trust services (QTS) conformity assessment against Regulation (EU) 910/2014

EY eIDAS QTSP/QTS certification scheme v1.3

As at 7 February 2020

Strictly confidential – Pending review

Building a better working world

CERTIFY EY POINT

Table of contents

1. Introduction

1.1 The eIDAS Regulation on eID and trust services

Regulation (EU) No 910/2014 (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.[1] 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 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 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, they are granted a higher presumption of their legal effect. For example, a 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.

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, fulfillment of the QTSP/QTS requirements and obligations. All of 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 the QTSP providing qualified time stamping services.

Before a trust services provider/trust service (TSP/TS) is granted a qualified status (QTSP/QTS), it will be subject to a pre-authorization 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 fulfills the eIDAS requirements. That audit must be conducted by a conformity assessment body specifically accredited to carry out assessments of a QTSP/QTS. The audit results in a formal conformity statement confirming — if such is the case — that the QTSP/QTS meets all of the applicable requirements of the eIDAS Regulation. Based on the notified information, including the report of such an audit, the competent SB will formally verify that the candidate QTSP/QTS meets the applicable eIDAS requirements and, in case of positive verification, it will undertake the publication of the grant of the qualified status for that QTSP/QTS in the national trusted list.

It is only when its qualified status is published in the corresponding national trusted list that the QTSP/QTS is authorized to provide the corresponding QTS. 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 that it meets requirements from Art.23 of the eIDAS Regulation (e.g., a link to the corresponding national trusted list where consumers may verify the granted qualified status must be displayed on the QTSP's website) and rules of the Commission Implementing Regulation (EU) 2015/806.[2]

Once granted a qualified status, QTSPs and their QTS have the obligation to pass and submit to the competent supervisory body a two-year conformity assessment report (CAR) issued by an accredited conformity assessment body (CAB) confirming that the QTSP and the QTS it provides fulfill the requirements laid down in the eIDAS Regulation. Competent supervisory

[1] See Article 3.16 of the eIDAS Regulation for the definition of trust services.

[2] 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. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2015.128.01.0013.01.ENG.

bodies are also allowed, at their own discretion and at any time, to themselves audit any QTSP/QTS for which they are competent, or to request an accredited CAB to perform an ad hoc audit.

QTSPs and their QTS are supervised for their entire life cycle, from their genesis to their termination. In particular, in order to ensure sustainability and durability of the QTS, as well as to ensure proper termination and a 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.

There are nine different types of QTS defined by the eIDAS Regulation for which a qualified status is granted separately: provisioning of qualified certificates for electronic signatures, provisioning of qualified certificates for electronic seals, provisioning 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.[3]

For more information and guidance on the QTSP/QTS initiation process, please refer to European Union Agency for Network and Information Security (ENISA) "Guidelines on initiation of qualified trust services."[4]

1.2 Accreditation and conformity assessment scheme under eIDAS

The requirements on CAB and the CAR referred to in Art.20.1, Art.20.1 and Art.21.1 are further specified by Art.3.(18) of the eIDAS Regulation that defines a "conformity assessment body" as "a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008,[5] 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." 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 fulfill 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 of the applicable requirements of the eIDAS Regulation.

The accreditation of CAB under eIDAS must ensure that conformity assessment activities used by such an independent body are such that there is a justifiable trust that the QTSP/QTS meet the requirements laid down in the eIDAS Regulation.

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 deemed appropriate) with the requirements of the eIDAS Regulation, while the supervisory body cannot refuse to grant the qualified status solely on the grounds that the proposed model does not comply with a given standard or a given business or technical model. QTSP/QTS are free to define the way to proceed to the implementation of the eIDAS-applicable requirements, whether operationally, organizationally or technically.

The normative requirements against which the conformity assessment scheme for which the CAB has been accredited under eIDAS and which the CAB uses to audit QTSP/QTS against the eIDAS Regulation are namely the requirements laid down in the eIDAS Regulation. It may be such that in addition to the conformity assessment, or certification when the conformity assessment scheme is a certification scheme and the CAB a certification body, the conformity assessment (or certification) scheme allows audited TSPs for being assessed (certified) against specific standards as a side result of the assessment (or certification) against the eIDAS Regulation requirement.

The eIDAS Regulation does not mandate compliance with any specific standard, and such compliance cannot be made mandatory for TSPs. However, it may be appropriate or even required for the notifying TSP intending to provide the QTS to ensure that it complies with specific standards in order to satisfy requirements in another application domain, provided they are not in contradicting 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

[3] See Annex 1 for more details.

[4] "ENISA Trust Services," *ENISA website*, https://www.enisa.europa.eu/topics/trust-services/guidelines, accessed 23 November 2020.

[5] 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.

CA/Browser Forum[6] requirements and requirements from Browsers or widely deployed applications owners for inclusion in their trusted certificate root stores.

Accreditation of CABs is an activity that under Regulation (EC) No 765/2008 is carried out by a single body in each of the EU Member States, called the national accreditation body (NAB). All NABs from EU Member States and from European Economic Area (EEA) countries are members of the European cooperation for Accreditation (EA), which is the body recognized under Regulation (EC) No 765/2008 that manages a peer assessment system among NABs from the EU Member States and other European countries. That rigorous and transparent peer assessment system ensures the equivalence of the accreditation services delivered by NABs and, thus, the equivalence of the level of competence of CABs. This mandatory peer assessment system facilitates the mutual recognition and promotes the overall acceptance of accreditation certificates and conformity assessment results issued by accredited bodies. National authorities shall recognize the equivalence of the services delivered by those accreditation bodies (i.e., the NABs), which have successfully undergone such peer assessment, and thereby accept the accreditation certificates of those bodies and the attestations issued by the CABs accredited by them.

Any CAB accreditation scheme and accredited conformity assessment scheme could be defined and used to accredit a CAB under the eIDAS Regulation, provided it meets the requirements of the eIDAS Regulation and, in particular, Art.3.18 and Art.20.1. Nevertheless, the EA has promoted the European Telecommunications Standards Institute (ETSI) EN 319 403 standard on requirements for CABs to carry out a conformity assessment of TSPs as one route to demonstrate conformity with relevant requirements of the eIDAS Regulation through assessment by accredited CABs. The EN 319 403 defined accreditation scheme is such that:

(i) It requires the accreditation of the CAB to be based on ISO/IEC 17065.

(ii) It supplements the general requirements provided in ISO/IEC 17065 to provide additional dedicated requirements for CABs performing certification of TSPs and the trust services they provide toward defined criteria against which they claim conformance.

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

(i) Take into account specificities of the type of trust service to be assessed

(ii) Ensure that all aspects of the TSP activity are fully covered

(iii) Be based on standards, publicly available specifications or regulatory requirements

Consequently, the EA-promoted accreditation scheme (ISO/IEC 17065 completed by ETSI EN 319 403) cannot be implemented unless such effective criteria and the related controls are clearly defined in a way that the NAB can evaluate the competency of the CAB to conduct an assessment of a QTSP/QTS against them in order to assess its conformity with the eIDAS requirements, and so that the accreditation cannot be contested. Their definition will be the purpose of the present document, namely the EY eIDAS QTSP/QTS certification scheme.

[6] 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 Secure Sockets Layer/Transport Layer Security (SSL/TLS), and code signing and has established guidelines to provide greater assurance to internet users about the websites they visit by leveraging the capabilities of SSL/TLS certificates. See www.cabforum.org.

2. Certification scheme

2.1 Objectives

The certification body of EY CertifyPoint is an accredited independent and impartial certification institute with experienced auditors all over the world certifying some of the top international organizations. It offers companies certification services for products, systems, services and processes in the area of information technology.

The certification is based on normative documents, such as legal regulations, standards or technical specifications, in which requirements for products and services are set out. Such certification by an independent third party enables companies to document that their products comply with the defined requirements.

The certification body of EY CertifyPoint is accredited for the certification of services on the basis of EN ISO/IEC 17065[7] as profiled by ETSI EN 319 403[8] and against the requirements defined in Regulation (EU) No 910/2014[9] (hereafter, the eIDAS Regulation).

2.2 Scope

Within the scope definition, we will refer to the following definitions of the eIDAS Regulation:

I. "Trust service" (Art.3.16) means an electronic service normally provided for remuneration, which consists of:
   a. The creation, verification and validation of electronic signatures; electronic seals or electronic time stamps; electronic registered delivery services; and certificates related to those services
II. Or
   a. The creation, verification and validation of certificates for website authentication
III. Or
   a. The preservation of electronic signatures, seals or certificates related to those services
IV. "Qualified trust service" (Art.3.17) means a trust service that meets the applicable requirements laid down in this Regulation.
V. "Trust service provider" (Art.3.19) means a natural or a legal person who provides one or more trust services either as a qualified or as a nonqualified trust service provider.
VI. "Qualified trust service provider" (Art.3.20) means a trust service provider that provides one or more qualified trust services and is granted the qualified status by the supervisory body.
VII. "Electronic signature creation device" (Art.3.22) means configured software or hardware used to create an electronic signature.
VIII. "Qualified electronic signature creation device" (Art.3.23) means an electronic signature creation device that meets the requirements laid down in Annex II.
IX. "Electronic seal creation device" (Art.3.31) means configured software or hardware used to create an electronic seal.
X. "Qualified electronic seal creation device" (Art.3.32) means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II.

We refer to article 3 of the eIDAS Regulation for definitions related to the regulation.

The scope of the certification scheme is defined as (qualified) TS and (qualified) TSP.

[7] ISO/IEC 17065:2012: Conformity assessment – Requirements for bodies certifying products, processes and services.

[8] ETSI EN 319 403 V2.2.2 (2015-08): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing TSPs. This document builds on ISO/IEC 17065 to specify additional requirements for CABs and additional auditing rules under which CABs will have to carry out their conformity assessments of QTSPs and their QTSs. "Requirements for conformity assessment bodies assessing Trust Service Providers," *ETSI website*, http://www.etsi.org/deliver/etsi_en/319400_319499/319403/02.02.02_60/en_319403v020202p.pdf, accessed 23 November 2020.

[9] 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. "Document 32014R0910," *EUR-Lex website*, http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG, accessed 23 November 2020.

The certification of qualified electronic signature creation and qualified electronic seal creation devices is out of the scope of the scheme.

The present document describes the certification scheme for the issuance of EY CertifyPoint certificates to TSPs, for the TS they provide within this accredited scope, and is intended to provide companies seeking certification by EY CertifyPoint with all necessary information.

2.2.1 Trust services

Based on the definition of TS by the regulation, we consider the following specific TS in the scope of the certification scheme:

- Provisioning of qualified certificates for electronic signatures
- Provisioning of qualified certificates for electronic seals
- Provisioning 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
- Qualified electronic registered delivery services

2.2.2 Qualified trust services

Within the certification scheme, we will refer to TS and TSP as QTS and QTSP, respectively, as the scheme refers to a TS or TSP that meets the applicable requirements laid down in the eIDAS Regulation.

Based on the definition of a QTS (Art.3.17), a conformity assessment will be performed to assess that a TS meets the applicable requirements laid down in the eIDAS Regulation.

Throughout the scheme, we will use the following naming for the TS that meets the applicable requirements in the eIDAS Regulation. We refer to Annex 1 of this document for the definition of the TS.

These have been based on guidance documents published by ENISA[10] and the related definitions in the ETSI standard[11] referenced by Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists.[12]

2.2.3 Signature and seal creation devices

The certification of qualified electronic signature creation and qualified electronic seal creation devices is out of the scope of the scheme. However, during the conformity assessment, if applicable according to the TS in scope, the certification of the qualified electronic signature or seal creation device must be thoroughly reviewed by:

1) Verifying the certificate of the certification

2) Reviewing the report of the certification

[10] Guidelines on initiation of qualified trust services v0.7, "Trust services guidelines," *ENISA website*, https://www.enisa.europa.eu/acl_users/credentials_cookie_auth/require_login?came_from=https%3A//www.enisa.europa.eu/topics/trust-services/guidelines/initiation_tsps, accessed 24 November 2020.

[11] ETSI TS 119 612 V2.2.1 (2016-04), "Trusted Lists," *ETSI website*, https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.02.01_60/ts_119612v020201p.pdf, accessed 24 November 2020.

[12] Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists, "Commission Implementing Decision (EU) 2015/1505," *European Commission website*, https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1505_en_txt.pdf, accessed 24 November 2020.

2.2.4 Regulatory environment

The certification scheme is based on the requirements of the eIDAS Regulation (Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and TS for electronic transactions in the internal market and repealing Directive 1999/93/EC).

In addition to the eIDAS Regulation, the following (EU) implementing acts (related to the eIDAS Regulation) apply:

- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means
- Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 on defining the circumstances, formats and procedures of notification
- Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 on the form of the EU Trust Mark for QTS
- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists
- 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 recognized by public sector bodies
- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices

National requirements

Even though the eIDAS Regulation is a regulation and therefore does not require national implementing laws in the EU Member States, the EU Member States are free to define implementing laws, define additional requirements, extend the regulation or align national laws with the regulation.

National requirements must be considered based on the country in which the TSP is located. It is important to consider and include the applicable national regulatory requirements during an eIDAS conformity assessment. The conformity assessment body must perform analysis of the national regulation applicable to an assessment during the preparation phase and define accurate test steps and criteria to verify conformity with these additional requirements.

For example, within the Netherlands, the eIDAS Regulation is implemented into national law through the following:

- Staatsblad 2017 – 75; Besluit van 22 Februari 2017, houdende vaststelling van eisen inzake verlening van vertrouwensdiensten, tot intrekking van het Besluit elektronische handtekeningen en tot aanpassing van enige andere besluiten (Besluit vertrouwensdiensten)[13]

Annex 2 of the certification scheme provides an indicative overview of national requirements and the impact on the conformity assessment.

2.3 Requirements for conformity assessment body (CAB)

We refer to the following definition of the eIDAS Regulation:

"Conformity assessment body" (Art 3.18) means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that regulation as competent to carry out a conformity assessment of a QTSP and the QTS it provides.

A certification body (in this case EY CertifyPoint) carrying out conformity assessments and certification against the present document must be accredited under ISO/IEC 17065 as complemented by ETSI EN 319 403. It shall conduct conformity assessments and certification against the present document in accordance with ETSI EN 319 403.

A conformity assessment is a type of audit. Based on the determination activity being of the type "audit," the CAB should comply with all requirements of ISO/IEC 17021-1. Section 10 – Option A is applicable.

[13] Besluit van 22 Februari 2017, houdende vaststelling van eisen inzake verlening van vertrouwensdiensten, tot intrekking van het Besluit elektronische handtekeningen en tot aanpassing van enige andere besluiten (Besluit vertrouwensdiensten).
"Besluit van 22 Februari 2017," *Overheid website*, http://wetten.overheid.nl/BWBR0039284/2017-03-10, accessed 24 November 2020.

2.4 Summary

The present scheme describes the requirements for certification of QTSP/QTS against the eIDAS requirements, including QTSP/QTS criteria, and the related controls, which should be efficient to demonstrate QTSP/QTS conformity with all of the eIDAS requirements, in such a way that:

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

The present scheme also allows separate certification of QTSP/QTS against specific standards as they are listed in Table 1.

The conformity assessments and certifications carried out under the present scheme document are carried out by EY CertifyPoint, a certification body accredited under ISO/IEC 17065, supplemented by ETSI EN 319 403, and providing additional dedicated requirements for CABs performing certification of TSP and the TS they provide toward defined criteria against which they claim conformance.

Table 1: Intended scope of accreditation

Product or product group to be certified	Certification scheme	Standard and normative documents

Qualified trust service provider (QTSP)
Trust services (TS) provided by a trust service provider (TSP)
Provisioning of qualified certificates for electronic signatures
Provisioning of qualified certificates for electronic seals
Provisioning of qualified certificates for website authentication
Qualified validation service for qualified electronic signatures
Qualified validation service for qualified electronic seals
Qualified preservation service for qualified electronic signatures
Qualified preservation service for qualified electronic seals
Qualified electronic time stamps services
Qualified electronic registered delivery services
	Name of the scheme:
	EY eIDAS QTSP/QTS certification scheme
	Methods of conformity assessment:
	ISO/IEC 17067 scheme type 6:
	- Initial review of TSP and TS design
	- Initial assessment of TSP and TS implementation
	- Initial assessment of TSP and TS operations
	- Surveillance:
	  - Assessment of TSP and TS design changes
	  - Assessment of the TSP and TS supporting processes
	  - Assessment of the TSP and TS operations
		Normative: eIDAS Regulation (EU) N°910/2014, including applicable implementing acts and national regulatory requirements
		Scheme: EY eIDAS QTSP/QTS certification scheme
		Supporting standards:
		- ETSI EN 319 102
		- ETSI EN 319 401
		- ETSI EN 319 411-1 and 411-2
		- ETSI TS 119 412-1 to 412-5
		- ETSI TS 103 171 to 174
		- ETSI EN 319 421
		- ETSI EN 319 422
		- ETSI TS 102 640-3
		- ETSI EN 319 521
		- ETSI EN 319 531
		- ETSI TS 119 495
		- ETSI TS 119 102-1
		- ETSI TS 119 441
		- ETSI TS 119 511

2.5 Maintaining the scheme

EY CertifyPoint is involved in the complete development and management aspects of the certification scheme.

During the development phase, a combination of team members knowledgeable about the domain of TS certification and other members of the team with experience in preparation for accreditation and indicating accreditation requirements provide input to create a coherent certification scheme.

During the development of the scheme, it was clear that the eIDAS Regulation, the relevant implementation acts and the national regulation are under development and updates to these requirements are performed on a regular basis.

The certification scheme should be maintained to reflect the relevant updates to the external requirements on which the scheme is built. This includes changes to the regulation or applicable standards.

Management of the certification scheme encompasses the activities of reviewing the scheme and providing approval for the usage of the scheme during certification activities.

2.6 Transitional arrangements

2.6.1 Transitions between the EY eIDAS certification scheme

A new version of the certification scheme will be applied, based on the selection of the newest version of the certification scheme during the preparation phase of the conformity assessment. As soon as the version is selected, the same version will be used throughout the complete conformity assessment. In case of an update to any of the standards mentioned in the scheme, clients are advised to switch to the latest version immediately; however, there is a transition period of a maximum of one year from a previous version of the scheme to the next version of the scheme.

2.6.2 Transition from other schemes

EY CertifyPoint is aware of related certification schemes within the domain of qualified certificates, such as the TTP.NL Scheme for management system certification of Service Providers issuing Qualified Certificates for Electronic Signatures, Public Key Certificates, and/or Time-stamp tokens.

If the TSP is in the possession of a certificate related to such a certification scheme, it will be noted by EY CertifyPoint. It will not be taken into account during a conformity assessment and will not in any way impact the activities of the conformity assessment as described in the EY eIDAS certification scheme.

2.7 Contact

In case of additional questions regarding the certification procedure, the certification body can be contacted as follows:

Cross Towers, Antonio Vivaldistraat 150
1083 HP Amsterdam, the Netherlands
Email: jatin.sehgal@nl.ey.com
Phone: +31 (0) 88 407 1000

2.8 Resources

This section details the relevant resources for the certification scheme and the complete file name for each resource.

Document	File name
Conformity assessment report	EY eIDAS Conformity Assessment report v6.docx
Audit plans	
T-15 Audit plan surveillance audit	T-15 Template Audit plan surveillance audit – v0.2_eIDAS.docx
T-7 Audit plan stage 1 audit	T-7 Template audit plan stage 1 audit – v0.2_eIDAS.docx
T-8 Audit plan stage 2 audit	T-8 Template audit plan stage 2 audit_v0.2_eIDAS.docx
Audit reports	
T-9 Audit report stage 1 audit	T-9 Template audit report stage 1 audit _v0.2_eIDAS.docx
T-16 Audit report surveillance audit	T-16 Template audit report surveillance audit – v0.2_eIDAS.docx
Application forms	
F-4	F-4 Application form – v5.6_eIDAS.docx
F-5a	F-5a Application Review form – EIDAS.docx
Competence requirements	
F-11a Competence requirements and qualification procedure for auditors	F-11a Initial evaluation form – Auditor requirements – v2 – Competence requirements and qualification procedure.docx
F-11b Competence requirements and qualification procedure for audit	F-11b Initial evaluation form – Audit requirements – v2 – Competence requirements and qualification procedure.docx
F-11c Competence requirements and qualification procedure for eIDAS	F-11c eIDAS requirements evaluation form – v1 – Competence requirements and qualification procedure.docx
Manuals and procedures	
General Procedures and Processes – ISO 17065 and eIDAS	Quality Manual for ISO 17065 and eIDAS scheme_v1.1.docx
Quality Manual – eIDAS	Quality procedures for CertifyPoint_v1.1.docx
Work plans	
EY eIDAS Certification Scheme – Requirements mapping guidance	EY eIDAS Certification Scheme – Requirements mapping guidance.docx
Provisioning of qualified certificates for electronic signature v1.3	Provisioning of qualified certificates for electronic signature v1.3.xlsx
Provisioning of qualified certificates for electronic seals v1.3	Provisioning of qualified certificates for electronic seals v1.3.xlsx
Provisioning of qualified certificates for website authentication v1.3	Provisioning of qualified certificates for website authentication v1.3.xlsx
Qualified preservation service for qualified electronic seals v1.3	Qualified preservation service for qualified electronic seals v1.3.xlsx
Qualified preservation service for qualified electronic signatures v1.3	Qualified preservation service for qualified electronic signatures v1.3.xlsx
Qualified validation service for qualified electronic seals v1.3	Qualified validation service for qualified electronic seals v1.3.xlsx
Qualified validation service for qualified electronic signatures v1.3	Qualified validation service for qualified electronic signatures v1.3.xlsx
Qualified electronic time stamp service v1.3	Qualified electronic time stamp service v1.3.xlsx
Qualified electronic registered delivery service v1.3	Qualified electronic registered delivery service v1.3.xlsx

3. Certification process

3.1 Overview

Achieving eIDAS certification of QTSP/QTS is a step-by-step process, as follows:

1) Preparation: This step consists of the TSP intending to provide a QTS and seeking for a conformity assessment (report) against the eIDAS requirements in the context of Art.21.1 of the eIDAS Regulation, or for the QTSP/QTS seeking for a conformity assessment (report) against the eIDAS requirements in the context of Art.20.1 or Art.20.2 to:

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

    b) Set up the relevant documentation. The documentation related to the provision of the QTS should be established in a way to support and facilitate the demonstration of conformity with the eIDAS requirement. TSPs should structure their documentation against the eIDAS requirements. The documentation should conform to the requirements of the present document and at least include:

        i) The risk assessment related documentation aimed to support demonstration of the requirement of eIDAS Art.19.1.
        ii) A security and personal data breach notification plan aimed to support demonstration of the requirement of eIDAS Art.19.2.
        iii) The termination plan (eIDAS Art.24.2.(i))
        iv) Declaration of practices, policies, security concept, procedures and guidelines the TSP will use to provide the QTS aimed to support demonstration of the other applicable eIDAS requirements

2) Conformity assessment: Before starting the audit, the TSP and the CAB will perform a set of preparation activities in order to define and agree on the audit plan and scope. This initial step will help set the timing of the audit, as well as the exact locations where the two stages of the audit will take place. Next to that, the CAB will establish the initial list of up-to-date documents regarding the (Q)TSP/(Q)TS, which are required to perform the conformity assessment.

    a) Stage 1: This stage focuses on obtaining and reviewing the documentation on the (Q)TSP/(Q)TS.

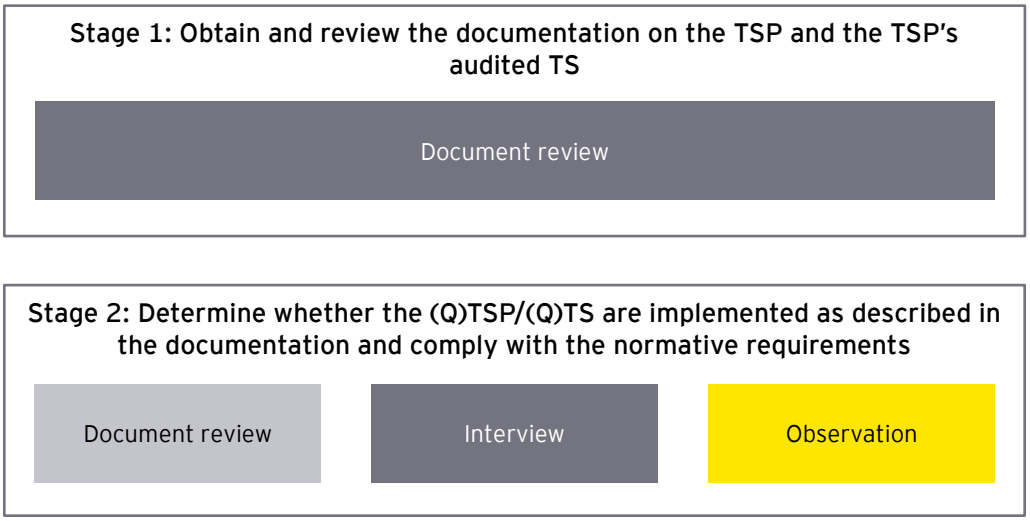
    b) Stage 2: This stage consists in an on-site audit that aims to validate the preliminary (Stage 1) audit report findings and to complete the audit of the (Q)TSP/(Q)TS against the assessment criteria.

    c) Conformity assessment report (CAR) and certification decision: At the end of the process, a CAR containing all of the results of the audit will be issued by the CAB to the (Q)TSP. In addition to a CAR, based upon a positive certification decision, a certificate will be issued.

    d) Surveillance assessments and recertifications: ETSI EN 319 403 under which the certification body of EY CertifyPoint (CAB) has been accredited recommends the CAB perform an annual surveillance audit in accordance with the provisions laid down in that standard. The eIDAS Regulation does not formally require such an annual surveillance assessment, but it requires in its Art.20.1 that QTSPs "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."

The following visualization provides an overview of the conformity assessment process.

Figure 1: Overview of the conformity assessment process



3.2 Documentation

The processes and procedures applicable to the certification process are documented within multiple documents. The current certification scheme provides information for applicable parties about the certification process by describing the relevant and public aspects of the process.

Refer to section 2.8 "Resources" for an overview of the related documents.

Several elements of the certification process are supported by internal processes and procedures, which are described in internal process and procedure documentation and quality manuals, enabling the integration of these elements in the internal processes and procedures applied by EY CertifyPoint.

3.3 Application

This process outlines the first step in the certification process, called "Application for Certification." It covers the high-level process and procedures for initiating a certification audit based on the request of a client.

When a client shows interest in becoming certified for compliance with the eIDAS Regulation, the first action to perform is gathering all required information. For this purpose, the process of the application is initiated. The application process supports the team in determining if the client is ready for certification and to initiate the entire certification process.

3.3.1 Process overview and activities

In this process, the certification body will perform a set of preparation activities aiming to define and agree on the plan and scope of the assessment. This initial stage will also help set the timing of the audit, the exact locations where the stages will take place, an assessment and certification proposal regarding the desired area of certification, and the assessment and certification agreement terms and conditions.

Once it is established that the client is eligible for certification, an application form (F-4) must be filled out to ensure all required information for certification is provided.

3.3.2 Review form

The central team will briefly review the application form to determine if sufficient information is available for performing a formal application review.

3.4 Application review

The purpose of performing an application review is to determine if sufficient information has been received from the client to prepare for the certification audit (or conformity assessment audit) and select an appropriate team. This allows the central team to determine the audit size for each location in scope in order to prepare a suitable proposal for the certification audit.

3.4.1 Process overview and activities

The process of performing an application review consists of several subprocesses.

3.4.2 Review the application form

Once the application form is received from the client, the central team shall review the form to determine if sufficient information is provided to determine the audit requirements. As part of the review, the following items shall be assessed in the F-5a form:[14]

- The information as provided about the client and the product is sufficient for the conduct of the certification process
- Areas of activity of the TSP and the associated business risk are understood
- Types of sites in scope
- Any known difference in understanding between the certification body and the client is resolved, including agreement regarding standards or other normative documents
- The scope of certification sought is defined (i.e., the TS and, if applicable, specific components in scope)
- The means are available to perform all evaluation activities
- The certification body has the competence and capability to perform the certification activity
- The availability of the required competencies can be confirmed

All details shall be documented in the Application Review form (F-5a) and used to determine if the appropriate competencies are available within EY CertifyPoint. The decision to undertake certification shall be justified in the Application Review form (F-5a).

If required, additional approval from the Committee of Impartiality shall be requested by the global quality manager through a request to the director. If either through Committee of Impartiality consultation or internal EY independence assessment or the unavailability of the competence it is determined that the client cannot be accepted, the central team will provide this feedback to the client. If the client is accepted, the evaluation activities shall be initiated.

3.4.3 Determine audit size

The time to be allocated for TSP audits will be based on following factors:

- The size of the TS scope (e.g., number of information systems used, number of employees, number of certificates issued)
- Complexity of the TS
- The type of business performed within scope of the TS
- Extent and diversity of technology utilized in the implementation of the various components of the TS
- The number of sites
- Previously demonstrated performance of the TS
- Extent of outsourcing and third-party arrangements used within the scope of the TS
- The standards, publicly available specifications and regulatory requirements that apply to the certification
- Existing certifications

The audit time as calculated using the above factors will be documented in a justification document or equivalent document for any initial audit, surveillance audits and recertification audit.

[14] Please refer to the documents listed under "Application form" in Section 2.8 "Resources."

3.4.4 Preparing the proposal

Based on the positive evaluation of a client certification application, a proposal will be prepared. This internal process is described in Section 4 of the "General Procedures and Processes - ISO 17065 and eIDAS" document.[15]

3.4.5 Certification efforts

The certification body of EY CertifyPoint shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or recertification audit. The time allocated shall be based on factors such as:

- The size of the TSP's organization (e.g., number of employees, number of information systems used)
- The complexity of the information and communication systems infrastructure (e.g., criticality of information systems, risk situation)
- The component TS performed
- The extent and diversity of technology used in the implementation of the various components of the TS (such as implemented controls, documentation or process control, corrective and preventive action, etc.)
- The number of sites where TS is operated or provided
- In case of surveillance and recertification audits, the previously demonstrated performance of the TSP/TS
- The extent of outsourcing and third-party arrangements used within the scope of the services
- The applicable normative requirements

The conformity assessment would usually be performed by a team of two or three auditors possessing knowledge and experience in the areas of Public Key Infrastructure (PKI) processes, information security and service provider management, in accordance with ETSI EN 319 403.

In general, the initial audit of a TSP/TS whose organization performs all service components in providing a specific TS would require an effort of 15 to 30 person days.[16]

To this, should be added one person day for application handling; a maximum of four person days for preparation; a maximum of four person days for audit reporting (stage 1 audit report and stage 2 audit report); and two person days for the review of audit reports, the certification decision and administrative follow-up.

The total number of person days required for the initial certification with all service components for a specific TS in scope would usually be in the order of 20 to 40 person days, depending on the complexity of the TS. Deviations from this guidance should be properly justified and recorded based on acceptable factors that may increase or reduce the assessment duration (see above).

An annual surveillance audit would take 5 to 15 person days, including the assessment preparation and reporting.

The above effort estimation is subject to variation in function, most notably the size and complexity of the TSP organization and implementation of the TS it provides, which could require visiting less or more locations with associated travel and extra reporting time.

The certification body of EY CertifyPoint shall document the reasons for the number of person days in its proposals to TSPs and should be able to present such information on request to the accreditation body.

3.4.6 Certification expenses

The expenses for carrying out assessments, certification and any related activities, when applicable, are indicated in the applicable terms and conditions of the certification body of EY CertifyPoint.

[15] Please refer to the documents listed under "Manuals and procedures" in Section 2.8 "Resources."

[16] The estimation is based on conformity assessment for one specific trust service.

3.5 Selection

3.5.1 Audit criteria

The scope of the audit criteria for the certification and conformity assessment is defined by a selection or combination of:

- Articles applicable to TS, as defined by the eIDAS Regulation and national regulations (see Section 2.2.4 "Regulatory environment")
- Standards (e.g., ETSI 319 401, 411-1)
- Reference material (French National Cybersecurity Agency (ANSSI) requirements)

3.5.1.1 Limited-scope certification and assessments

Subsets of activities are often outsourced to other trust service providers, which then perform only a limited set of activities in the context of the TS (i.e., component services).

For example, provider A performs registration authority activities as part of provisioning qualified certificates for provider B.

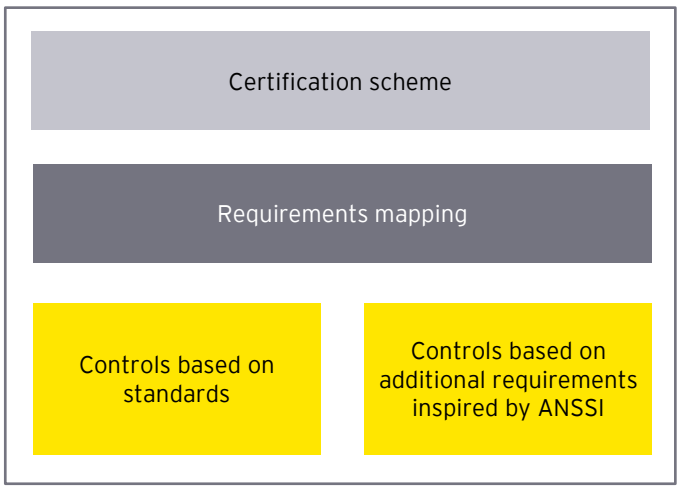
It is not mandatory to cover the full scope of a trust service, standard or reference material during certification and assessment. TS providers that perform a subset of activities in the context of a TS must clearly indicate the scope of their activities.

The same approach applies for TS providers looking for certification of specific standards, considering all or part of the standards (e.g., 319 401, 411-1 and 411-2) in scope.

The certification and assessment scope will then be limited to these activities and reporting will clearly indicate the boundaries of the certification and assessment.

3.5.1.2 Standards and reference material

The eIDAS Regulation does not mandate compliance with a specific standard. However, standards can provide controls that allow for specific elements of the normative requirements to be verified or tested, thereby assisting the conformity assessment team in assessing the conformity with a requirement of the regulation.



The standards or reference material are subject to changes, for example, if a new version of the standard is published. Please refer to the document "EY eIDAS Certification Scheme – Requirements mapping guidance" for the approach to covering the eIDAS requirements through a combination of ETSI standards and additional requirements inspired by ANSSI.

Refer to Annex 4 for the mapping of articles, standards and reference material.

3.5.1.3 Policies

In addition to standards, specific policies as defined within ETSI standards can be selected to further clarify the scope of the requirements that are applicable.

3.5.2 Preparing the conformity assessment process

Upon conclusion of the certification contractual agreement, the certification body of EY CertifyPoint will request that the TSP makes all necessary arrangements for the conduct of the audit, including the provision for examining documentation and the access to all areas, including those of subcontractors, records (including internal audit reports and reports of independent reviews of information security) and personnel for the purposes of the audit, recertification audit and resolution of complaints.

3.5.2.1 Team selection

The auditors that perform the EY CertifyPoint audits must have the proper technical skill set, qualifications and experience to successfully perform certification audits. It is crucial that the EY CertifyPoint central team can guarantee the quality of new members and local resources at EY member firm offices around the globe.

For each audit, auditors and technical professionals will be:

a) Selected based on the basis of their competence, training, qualifications and experience

And

b) Monitored for the performance during audits

Requirements toward competencies and experience have been defined in forms (F-11a, F-11b and F-11c)[17] for personnel involved in the certification process, based on the requirements of ISO 17065 and ETSI 319 403. Every member involved in the certification process will fill in the applicable competence and qualification forms, describing competencies and experiences.

3.5.2.2 Preparing and sending the audit plan

To make certain of the preparedness of both the auditors and the client, an audit plan will be sent to the client prior to the audit. This process provides guidance for the team about preparing and sending the audit plan to the client.

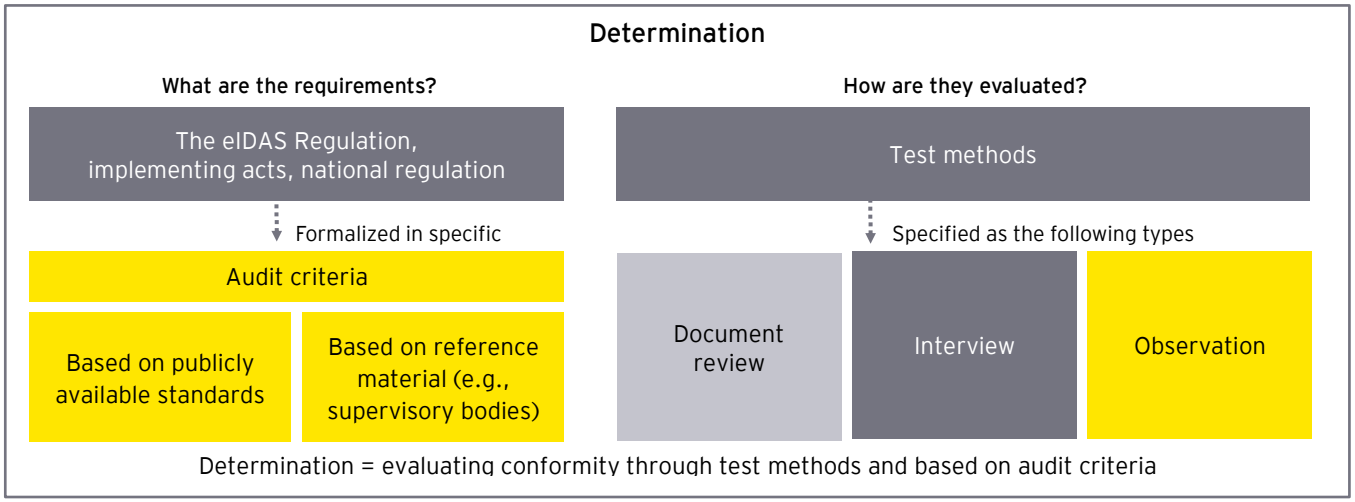
3.6 Determination

Upon the conclusion of the certification contractual agreement, the certification body of EY CertifyPoint will assign a certification process number and inform the contracting TSP of the name of the responsible certifier and the responsible team leader. The responsible certifier and the auditors agree with the TSP the time schedule of the certification process.

3.6.1 Overview

The following visualization provides an overview of the determination activities.

Figure 2: Overview of the determination activity



[17] Please refer to the documents listed under "Competence requirements" in Section 2.8 "Resources."

3.6.2 Performing the audit process

The assessment is performed by the team under the responsibility of the team leader according to the requirements and specifications of the certification body. The responsible certifier, together with the TSP and the team, plans the time schedule of the assessment and certification process and, if necessary, finally clears any questions regarding the assessment and certification process in preliminary meetings.

The assessment comprises all activities that are necessary to obtain complete information about the fulfillment of the specified requirements by the certification object. That includes planning and preparation activities, as well as document review, observation and interviews.

The auditors audit the (Q)TSP/(Q)TS regarding their compliance with the relevant requirements of the eIDAS Regulation in consideration of the requirements of the standards. During such audit, compliance of the organizational and technical measures of the (Q)TSP/(Q)TS is assessed against the applicable requirements.

The assessment is organized under a two-stage audit process in accordance with ETSI EN 319 403.

- Stage 1: the documentation review
- Stage 2: the on-site audit

Upon completion of the assessment, the auditors prepare a conformity assessment report according to Art.20.1 of the eIDAS Regulation forming the basis of the certification decision. The certification body performs a review of the assessment using the prepared conformity assessment report and monitors compliance with the procedural requirements on the basis of ISO/IEC 17065 completed by ETSI EN 319 403. The certification decision is recorded. The TSP is informed about the decision.

The audits are performed by auditors who are either employees of the certification body of EY CertifyPoint or are persons approved by the certification body.

In case of a positive certification decision, the certificate is issued and reflects the scope of the certification and a validity period of two years maximum, and depicts the certification mark. A valid certificate authorizes the holder to publicly use the certification mark in connection with the certified QTS according to the EY certification agreement terms and conditions.

The certification body EY CertifyPoint performs its activities predominantly on the premises of EY CertifyPoint in Amsterdam. In addition, document reviews, observations and interviews are also performed on the TSP's premises or on any premises used by the TSP to provide its TS, in accordance with ETSI EN 319 403, in particular for multi-site sampling.

3.6.3 Determination activities

3.6.3.1 Definitions

In this section, we refer to the following definitions of ISO 17000:

I. (2.1) **Conformity assessment,** demonstration that specified requirements (3.1) relating to a product (3.3), process, system, person or body are fulfilled

   Note 1: The subject field of conformity assessment includes activities defined elsewhere in this ISO, such as testing (4.2), inspection (4.3) and certification (5.5), as well as the accreditation (5.6) of conformity assessment bodies (2.5).

II. (3.1) **Specified requirement,** need or expectation that is stated

   Note: Specified requirements may be stated in normative documents, such as regulations, standards and technical specifications.

III. (3.2) **Procedure**, specified way to carry out an activity or a process [ISO 9000:2000, 3.4.5]

IV. (3.3) **Product,** result of a process [ISO 9000:2000, 3.4.2]

   Note: Four generic product categories are noted in ISO 9000:2000: services (e.g., transport), software (e.g., computer program, dictionary), hardware (e.g., engine, mechanical part) and processed materials (e.g., lubricant). Many products comprise elements belonging to different generic product categories. Whether the product is then called service, software, hardware or processed material depends on the dominant element.

V. (4.1) **Sampling,** provision of a sample of the object of conformity assessment, according to a procedure (3.2)

VI. (4.2) **Testing**, determination of one or more characteristic of an object of conformity assessment, according to a procedure (3.2)

Note: "Testing" typically applies to materials, products or processes.

VII. (4.3) **Inspection**, examination of a product design, product (3.3), process or installation and determination of its conformity with specific requirements or, on the basis of professional judgment, with general requirements

Note: Inspection of a process may include inspection of persons, facilities, technology and methodology.

VIII. (4.4) **Audit**, systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements (3.1) are fulfilled

Note: While "audit" applies to management systems, "assessment" applies to conformity assessment bodies, as well as more generally.

3.6.3.2 Determination activity type

ISO/IEC 17065 (7.4.3) states that, "The certification body shall ensure all necessary information and/or documentation is made available for performing the evaluation tasks."

Note: The evaluation tasks can include activities such as design and documentation review, sampling, testing, inspection and audit.

The evaluation activities or tasks to be performed during the conformity assessment are of the determination activity type **audit**.

We consider the following evaluation activities or tasks as part of the **audit** activity type, as defined by ISO 17021-1 (Section 9.4.42):

1) Interviews
2) Review of documentation and records
3) Observation of processes and activities

3.6.4 Documentation request

Throughout the conformity assessment, the following documents will typically be required to be provided by the client for assessment:

- General information concerning and describing the TS and the activities it covers
- Description of the organizational structure of the TSP, including the use made and organizational structure of other parties (subcontractors) that provide parts of the TS being audited
- Description of the locations, sizes and functions (tasks and responsibilities) of roles and people involved in the TS operational life cycle processes, facility, management, technical security control processes (including other parties used, e.g., subcontractors), and also evidence of their competence or any analysis done for the same
- TS policy (e.g., certificate policy, time stamping policy) and TS practices statement (e.g., certification practices statement, time stamping practices statement) and, where required, the associated documentation like IT network infrastructure plans with all relevant systems, manuals and instructions for the operation of the TS
- The risk assessment related documentation aimed to support demonstration of the requirement of eIDAS Art.19.1, including:
  - Information security risk analysis with risks and opportunities and the actions taken to address them related to all of the interested parties
  - Description of the risk assessment and treatment methodology
- Management (in particular, policy management authority, or PMA) review and meeting minutes
- Internal and external audit reports or certifications
- Independent reviews of information security
- A security and personal data breach notification plan aimed to support demonstration of the requirement of eIDAS Art.19.2
- Evidence of the detection of and reaction to security incidents; nonconformities identified during external or internal audits, including the corrective action taken for each

- Network overview diagrams supporting segmentation and security measures
- Detailed verification steps and guidelines documentation
- Training materials for vetting staff
- Arrangements to cover liability (certificate and evidence of payment)
- Information security policies and procedures, including, but not limited to:
  - Key management
  - Logical security
  - Personnel security
  - Physical security
  - Backup and recovery
  - Incident management
  - Business continuity and disaster recovery
  - Data protection and asset classification
  - Change management
- Procedures and controls in support of:
  - Publication and repository responsibilities
  - Identification and authentication, when applicable
  - TS life cycle operational requirements
  - Facility, management and operation controls
  - Technical security controls
- The termination plan of TS (eIDAS Art.24.2.(i))
- Subscriber agreement and related terms and conditions

3.6.5 Stage 1 audit

In preparation for the audit, auditors shall obtain and review the documentation on the TSP and the TSP's audited TS. Auditors shall make the TSP aware of any further types of information and records that may be additionally required for verification during audit stage 1. In this stage of the audit, the CAB shall also obtain documentation of the design of the TS.

The objectives of the stage 1 audit are:

- To audit and review the (Q)TSP/(Q)TS documentation
- To evaluate (Q)TSP locations and site-specific conditions
- To provide a focus for planning the stage 2 audit by gaining an understanding of the structure and extent of the TSP's audited TS
- To review (Q)TSP status and understanding regarding requirements of the normative requirements and specifically those of the eIDAS Regulation, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the Ts
- To collect necessary information regarding the scope of the TS, processes and locations of the (Q)TSP; levels of controls established and related statutory and regulatory aspects and compliance (e.g., quality, environmental, legal aspects of (Q)TSP operation, associated risks)
- To perform verification of records regarding legal entity, arrangements to cover liability, contractual relationships between TSP and potential contractors operating or providing sub-component services, and further investigations with regard to the preliminary audit of the self-declared partial compliance or noncompliance
- To evaluate the effectiveness of the TS management to make certain the (Q)TSP is continually meeting its specified objectives
- To evaluate if the internal audits and management review are being planned and performed and that the level of implementation of TS management substantiates that (Q)TSP is ready for the stage 2 audit

During the first stage of the assessment of the (Q)TSP, the auditors analyze and examine the conformity of the documentation required by the normative requirements. If the assessment reveals that the (Q)TSP/(Q)TS described by the audited organization do not meet the requirements, no on-site audit is performed. The (Q)TSP is given the opportunity then to adjust the documentation to the requirements and have it examined by the auditors again.

If, after the examination of the (Q)TSP documentation, the auditors arrive at the conclusion that the (Q)TSP/(Q)TS with their documentation meet the requirements of the applicable normative requirements, the on-site audit is performed as the second stage of the assessment process.

Stage 1 reports shall be submitted by the team leader to the certification body of EY CertifyPoint. In combination with information held on file, these reports shall at least contain:

- A description of the organizational structure of the TSP/TS, including the use made and organizational structure of other parties (subcontractors) that provide parts of the TS being audited
- A brief summary of the document review
- An account of the audit of the information security risk analysis of the TSP and its TS being audited
- A brief assessment of the auditor whether stage 2 is likely to succeed and whether additional resources (e.g., technical professionals, more auditors) are required for stage 2
- Audit time spent on document review
- Any areas of concern about whether the TSP and its TS being audited meet the requirements of the applicable audit criteria
- The audit methodology employed for stage 1

In every case, the document review shall be completed prior to the commencement of audit stage 2. The results of audit stage 1 shall be documented in a written report, including any recommendations regarding planning for conducting the audit stage 2. The stage 1 audit findings, including identification of any areas of concern that could be classified as nonconforming during the stage 2 audit, shall be communicated to the TSP during the closing meeting of the stage 1 audit.

The audit report of the stage 1 audit will be sent to the subject-matter professional of EY CertifyPoint, who will decide on the readiness of the TSP for the start of the stage 2 audit. In determining the interval between stage 1 and stage 2 audits, consideration shall be given to the needs of the TSP to resolve areas of concern identified during the stage 1 audit. The certification body shall make the TSP aware of assessment audit stage 2 planning and of the further types of information and records that may be required for detailed verification during audit stage 2.

3.6.6 Stage 2 audit

The aim of this stage 2 audit is to determine whether the (Q)TSP/(Q)TS are implemented as described in the documentation and comply with the normative requirements. The on-site audit is performed on the premises of the TSP on a date agreed with the client in advance.

- The objectives of audit stage 2 are:
  - To confirm that the TSP adheres to its own policies, objectives and procedures
  - To confirm that the implemented TS conform to the requirements of the applicable audit criteria and abide by the applicable TSP's policies, objectives and procedures
- To do this, the audit will focus on collecting evidence of the TSP's TS with respect to:
  - Implementation of TS requirements
  - TS-related organizational processes and procedures
  - TS-related technical processes and procedures
  - Implemented information security measures for TS, including IT network protection
  - TS service-related products (trustworthy systems), such as cryptographic modules And
  - Physical security of the relevant TSP sites

The on-site audit includes the evaluation of the organizational, structural and technical implementation of the measures described in the documentation for fulfilling the applicable normative requirements.

To this end, auditors gather evidence by document review, observation and interview. The TSP's own declarations or test results for which no proof exists that they have been performed according to the requirements of the scheme may not be used as evidence.

To the extent available, also evaluations of other independent bodies regarding individual components of the service to be audited may be used. For instance, it is not necessary that auditors perform their own evaluations of technical components. They may use test reports and certificates of other independent bodies for their own evaluation. The responsible certifier

and the auditor shall agree upon the reuse extent, ensuring that reused results are applicable for the certification of the compliance of the (Q)TSP/(Q)TS against the normative requirements.

3.6.7 Audit criteria

The evaluation of the TSP and the TS it provides shall take the form of an audit carried out against defined criteria that:

a) Take into account specificities of the type of TS to be assessed

b) Ensure that all aspects of the TSP activity are fully covered

And

c) Are based on standards, publicly available specifications or regulatory requirements

The detailed controls are specified in work plans (listed in Section 2.8 "Resources"). These also indicate the recommended determination activity for each of the controls.

3.6.8 Evaluation

For each of the determination activity types, we define rules to allow the auditor to determine whether a control can be considered effective or ineffective (i.e., a finding).

3.6.8.1 Interview

A control that is covered through an interview should be considered effective if the interview provides sufficient evidence that the control is in place and performed according to the definition of the control requirements through a detailed description, such as (if applicable): a walk-through of how the control is performed, who performed the control and a description of the process in which the control is present.

A control that is covered through an interview should be considered ineffective if the interview is not able to provide evidence that the control is in place or that it is performed according to the definition of the control or its requirements.

3.6.8.2 Review of documentation and records

A control that is covered through a review of documentation or records should be considered effective if the review provides sufficient evidence that the control is in place and performed according to the definition of the control requirements through a detailed description, such as (if applicable): a detailed explanation of the control or the process in which the control is present or evidence that a control was performed (e.g., based on logs or audit records).

A control that is covered through a review of documentation should be considered ineffective if the review is not able to provide evidence that the control is in place or that it is performed according to the definition of the control or its requirements.

3.6.8.3 Observation of processes and activities

A control that is covered through observation of processes and activities should be considered effective if the observation (of the auditor) provides sufficient evidence that the control is in place and performed according to the definition of the control requirements through a detailed description, such as (if applicable): an observation that a control is performed (e.g., through on-site observation) within a process.

A control that is covered through observation of processes and activities should be considered ineffective if, during observation, there is insufficient evidence that the control is place or that it is performed according to the definition of the control or its requirements.

3.6.9 Sampling methodology

The selection size is based on a number of criteria, namely:

- The frequency of the control (see table below)
- The nature of the control (process controls should be subject to more extensive testing than, for example, configured controls)
- The importance of the control (controls that are relatively more important should be tested more extensively)

Furthermore, the extent of testing (selection size) depends on the risk failure of the control that is being tested. Factors that affect the risk failure are, for example, changes in the design of controls, changes in key personnel who perform the control and the complexity of the control.

The extent of testing (selection size) is a matter of professional judgment; however, the following table indicates the minimum selection size. Based on the risk of failure the selections, the size can be increased.

The sampling approach must always be chosen so that it supports the trustworthiness of the conformity assessment.

Frequency of control	Description	Selection
Multiple times per day	The control is performed more frequent than daily.	25
Daily	The control is performed on a daily basis.	25
Weekly	The control is performed on a weekly basis.	5
Monthly	The control is performed on a monthly basis.	2
Quarterly	The control is performed on a quarterly basis.	1
On occurrence	The control is performed when the described situation occurs.	10% of the population or 25 (as maximum)
Automated control	The control is not performed as such, but is continually present.	At least 1

3.6.9.1 Multi-site sampling

Where the client (or organization) has a number of sites, the team will consider using a sample-based approach to a multiple-site audit based on the following requirements:

a) Security for all applicable site is administered under control of the organization's security policy administration

And

b) All applicable sites are subject to the organization's security management review program

The following shall be considered during sampling of sites:

- Type of different sites as per application review form
- A representative number of sites to be sampled, taking into account:
  - The results of internal audits of the central site and the other sites
  - The results of management review
  - Variations in the size of the sites
  - Variations in the business purpose of the sites
  - Complexity of the trust service
  - Complexity of the information systems at the different sites
  - Variations in working practices
  - Variations in activities undertaken
  - Potential interaction with critical information systems or information systems processing sensitive information
  - Whether the site is operated by a subcontractor or other external organization
  - Any differing regulatory requirements
- Sample will be partly selective based on the above points and partly nonselective and result in a range of different sites being selected without excluding the random element of site selection
- Every site of the organization subject to significant threats to assets, vulnerabilities or impacts should be included in sampling program
- Surveillance program shall be designed in the light of the above requirements and shall, within a reasonable time, cover all site operations, unless it can be demonstrated this does not impact the results of the audit

  And
- In case of nonconformity being observed, either at the head office or at a single site, corrective action procedure shall apply to the head office and to all sites of the operations that may be impacted by the same nonconformity

The audit shall address the TSP's central site activities to make certain that central security administration is applied to all sites at the operational level.

A justification memo or equivalent document shall be used justify the number of sites being sampled in the audit.

3.7 Review

3.7.1 Conformity assessment report

Upon completion of the on-site audit, the auditors prepare a CAR according to Art.20.1 of the eIDAS Regulation on the basis of the documentary examination and the on-site audit with a statement about the compliance of the TS with the relevant normative requirements. This report forms the basis for the certification decision.

The certification decision is made by the management of the certification body of EY CertifyPoint and documented in the protocol on the certification decision.

The template for the conformity assessment report according to Art.20.1 of the eIDAS Regulation produced by the certification body of EY CertifyPoint is provided as an external document.

3.8 Decision

3.8.1 Certification decision

The certification decision is made by the management of the certification body of EY CertifyPoint and can be one of the following three natures:

a) **Certified:** The audited trust service fulfills the criteria and is certified as conforming

b) **Conditional:** A TSP audit may be passed with pending nonconformities, provided that these do not impact the ability of the TSP to meet the intended service. This certification decision is conditional upon to the implementation of corrective actions within three months after conclusion of the audit (depending on the type and criticality of the corrections)

Or

c) **Not certified**: The audited trust service is not certified as conforming.

3.8.2 Certification documentation

At the end of the process, a conformity assessment report containing all of the results of the audit will be issued by the CAB to the (Q)TSP. The conformity assessment report forms the basis for the certification decision.

In case of a positive certification decision, a certificate is issued and reflects the scope of the certification and a validity period of two years maximum, and depicts the certification mark. A valid certificate authorizes the holder to publicly use the certification mark in connection with the certified QTS, according to the Ernst & Young CertifyPoint BV certification agreement terms and conditions.

3.8.3 Findings

EY CertifyPoint rates the findings based upon the risk they pose to the TSP organization.

Guidance for the classification of the findings is as follows:

1. Minor nonconformity – a single identified gap or a concern in meeting a requirement of the standard, which would not in itself raise significant doubt as to the capability of the TSP to achieve its objectives
2. Major nonconformity – an absence of, or the repeated failure to implement and maintain one or more required mandatory standard element, or a situation that would, on the basis of objective evidence, raise significant doubt as to the capability of the TSP to achieve its objectives

In case findings are noted by the certification body during a conformity assessment, the certification body will follow up that the TSP organization takes the necessary measures to remediate these findings (may be performed through a surveillance audit).

3.8.4 Directory of certified products

EY CertifyPoint will maintain a directory of products that it has certified. It will make the directory publicly accessible with up-to-date information about certified TSPs and the certified TS they provide.

3.9 Changes affecting certification

There can be instances in which certain changes can impact the certification of the organization, such as:

- When the certification scheme introduces new or revised requirements that affect the client, EY CertifyPoint will make certain these changes are communicated to all clients. EY CertifyPoint will verify the implementation of the changes by its clients and will take action required by the scheme.
- When changes affecting certification are initiated by the client, due to major changes in documentation, policies, objectives, etc., or security-relevant changes, it is the responsibility of the client to provide notification of the change, as agreed to within the certification agreement.

A full recertification of the TSP's TS will be performed under the following circumstances:

- Whenever there are major changes to the scope
- Whenever there are major changes to the TS provided under the scope
- Whenever a new TS is included in the scope
- When there are major changes of IT systems or business processes used by the TSP

  Or
- When a major part of the TS moves to another location

Appropriate actions will be taken to implement changes affecting the certification in accordance with the defined processes.

3.10 Conditions on expiration, suspending, withdrawing or reducing scope of certification

EY CertifyPoint will suspend certification in cases when, for example:

- The client's certified service has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the management system, which is indicated in the report following a surveillance audit or recertification audit.
- The certified client does not allow surveillance or recertification audits to be conducted at the required frequencies.

  Or
- The certified client has voluntarily requested a suspension.

3.11 Attestation

3.11.1 Publication of certificates and use of certification marks

To support the transparency of certifications, the certification body maintains a list of the certified products and services, which is made available to the public. New certificates are published on the webpages at short notice after a positive certification decision has been made.

The certified TSP is entitled to use the certificate and the certification mark in connection with the certified product and service in publications, catalogs, etc., in compliance with the certification conditions of the certification body of EY CertifyPoint. In case of an incorrect reference or misleading use by the certified TSP of the certificate or any certification mark, the certification body is entitled to withdraw the certificate. The use of certification marks is formally described in the certification agreement.

Regularly monitoring the compliance of the certified TSP's use of the certificates and certification marks with the applicable terms and conditions is performed by the certification body of EY CertifyPoint.

3.11.2 Complaints and appeals

The complaints and appeals procedures are publicly available on the website of EY CertifyPoint.

3.12 Surveillance

The scheme provides the following guidelines for evaluating the need for a surveillance audit:

1) The TSP is required to inform the certification body immediately about all changes affecting the TS environment and provide a description of these changes. Based on the severity of these changes, the CAB must evaluate the need for a surveillance audit by evaluating the risk of major changes impacting the certification.
2) If an initial conformity assessment was performed for one or more new TS (i.e., the initial conformity assessment was the first conformity assessment for the service), it is recommended that a surveillance audit be performed.
3) A surveillance audit must be performed in case exceptions (at least one major or minor nonconformity) are identified during the previous conformity assessment.
4) The supervisory body of the applicable EU Member State must be consulted to align the expectations of performing an intermediate surveillance audit. A surveillance audit must be performed in the case of a request by the supervisory body.
5) In line with ETSI TS 119 403-2, a full surveillance audit shall be conducted no less frequently than annually for TSPs that issue publicly trusted certificates.

It is recommended that a surveillance audit be performed within the last half year of the first year after the issuance of the certificate to extend or maintain the validity of the certificate.

Similar to the initial audit, this surveillance audit is performed in accordance with the surveillance activities defined by ISO/IEC 17067 scheme type 6, through document review, observation and interviews. The sample is to be designed such that all changes and modifications that have been implemented since the time of the last audit are covered.

The activities to be performed during the different types of audits and assessments are detailed in the applicable audit plans (T-7, T-8 and T-15).[18]

At the maximum, one surveillance audit is permitted. After no more than two years, a complete audit to renew the validity of the certificate is required, according to Art.20.1 of the eIDAS Regulation.

[18] Please refer to the documents listed under "Work plans" in Section 2.8 "Resources."

4. Annex 1 – Qualified trust services defined by the eIDAS Regulation

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

4.1 Provisioning of qualified certificates for electronic signatures

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

A qualified electronic certificate for electronic signatures is an essential element for a signatory to create qualified electronic signatures that shall have the equivalent legal effect of a handwritten signature all over the EU.

4.2 Provisioning of qualified certificates for electronic seals

As explained above, since 1 July 2016, legal persons cannot create legally valid (qualified) electronic signatures anymore and cannot be issued (qualified) certificates for electronic signatures. Instead, legal persons can use certificates for electronic seals, which are electronic attestations that link electronic seal validation data to a legal person and confirm the name of that person. The aim of an electronic seal is not to sign, but to serve as evidence that an electronic data or document was issued by a legal person, providing certainty of the data's or document's origin and integrity.

A qualified electronic certificate for electronic seals is an essential element for a legal person to create qualified electronic seals that shall enjoy, all over the EU, the presumption of integrity of the data and the correctness of the origin of that data to which the qualified electronic seal is linked.

4.3 Provisioning of qualified certificates for website authentication

Certificates for website authentication are issued to make certain to the users (in particular, citizens and subject-matter experts) that behind the website there is a legal or natural person identifiable by trustworthy information.

The regulation sets clear requirements for qualified website authentication certificates to be considered trustworthy, together with the obligations for QTSPs of such qualified certificates with regard to the security of their operations, their liability and their supervision regime. As a consequence, the regulation provides transparency regarding the quality of the service offered to users, the accountability of providers with regard to the security of their services, the trustworthiness of the data associated with qualified authenticated websites, and the technological neutrality of the services and solutions.

4.4 Qualified preservation service for qualified electronic signatures

Such a qualified TS aims to provide the long-term preservation of information in order to make certain of the legal validity and trustworthiness of qualified electronic signatures over extended periods of time and to guarantee that they can be validated, regardless of future technological changes.

4.5 Qualified preservation service for qualified electronic seals

Such a QTS aims to provide the long-term preservation of information in order to make certain of the legal validity and trustworthiness of qualified electronic seals over extended periods of time and to guarantee that they can be validated, regardless of future technological changes.

4.6 Qualified validation service for qualified electronic signatures

Validation of an electronic signature is an ancillary service to electronic signatures, whose process aims to confirm the validity of an electronic signature.

Qualified validation services for qualified electronic signatures entail the verification by a QTSP that the requirements of the eIDAS Regulation are met by a qualified electronic signature in order to confirm its validity.

4.7 Qualified validation service for qualified electronic seals

Validation of an electronic seal is an ancillary service to electronic seals, whose process aims to confirm the validity of an electronic seal.

Qualified validation services for qualified electronic seals entail the verification by a QTSP that the requirements of the eIDAS Regulation are met by a qualified electronic seal in order to confirm its validity.

4.8 Qualified electronic time stamps services

Electronic time stamps are issued to make certain of the correctness of the time linked to data and documents.

A 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.

4.9 Qualified electronic registered delivery services

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

The regulation sets clear requirements for all such QTS to be considered trustworthy, together with the obligations for their QTSPs with regard to the security of their operations, their liability and their supervision regime.

5. Annex 2 – National requirements

5.1 The Netherlands

5.1.1 National implementing law

Staatsblad 2017 – 75; Besluit van 22 Februari 2017, houdende vaststelling van eisen inzake verlening van vertrouwensdiensten, tot intrekking van het Besluit elektronische handtekeningen en tot aanpassing van enige andere besluiten (Besluit vertrouwensdiensten)[19]

5.1.2 Impact on conformity assessment

Section 2, Article 2, "Kennisgeving inbreuk veiligheid of verlies integriteit," defines additional requirements related to Art.19.2 of the eIDAS Regulation. Conformity with these requirements must be assessed during the conformity assessment.

Section 3, article 3, "Aanwijzing certificerende instellingen gekwalificeerde middelen aanmaken elektronische handtekeningen," is not applicable since the certification of qualified electronic signature or seal creation devices is not in the scope of the scheme (see section 2.2.3 "Signature and seal creation devices").

5.2 Belgium

5.2.1 National implementing law

21 Juli 2016 – Wet tot uitvoering en aanvulling van de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, houdende invoeging van titel 2 in boek XII "Recht van de elektronische economie" van het Wetboek van economisch recht, en houdende invoeging van de definities eigen aan titel 2 van boek XII en van de rechtshandhavingsbepalingen eigen aan titel 2 van boek XII, in de boeken I, XV en XVII van het Wetboek van economisch recht.[20]

[19] Besluit van 22 Februari 2017, houdende vaststelling van eisen inzake verlening van vertrouwensdiensten, tot intrekking van het Besluit elektronische handtekeningen en tot aanpassing van enige andere besluiten (Besluit vertrouwensdiensten). "Besluit van 22 Februari 2017," *Overheid website*, http://wetten.overheid.nl/BWBR0039284/2017-03-10, accessed 24 November 2020.

[20] "21 Juli 2016," *European e-Justice website*, http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?imgcn.x=70&imgcn.y=12&DETAIL=2016072140%2FN&caller=list&row_id=1&numero=1&rech=&cn=2016072140&table_name=WET&nm=2016009485&la=N&sql=dd+%3D+date%272016-07-21%27+and+nm+contains+%272016009485%27&language=nl&tri=dd+as+rank&fromtab=wet, accessed 24 November 2020.

6. Annex 3 – Trusted list

Article 22 of the eIDAS Regulation states, "Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them."

Therefore, the responsibility of maintaining the trusted lists is owned by the EU Member State. However, as it requires information related to the QTSPs and the related QTS provided by them, within the CAR, we provide input to the supervisory body for the trusted list entry.

Section 1.3.2 "Trust service" of the CAR defines the scope of the conformity assessment and the TS hierarchy providing this TS. If applicable, the "service digital identifier," "additional service information," "Qualified Signature Creation Device (QSCD)" and other relevant TS field values are specified.

6.1 Format and specifications

Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists,[21] defines the technical specifications and formats of the trusted lists and relies on ETSI 119 612 v2.1.1 for specifications and requirements.

6.2 Example contents

The scope of the conformity assessment has been defined as covering the "provisioning of qualified certificates for electronic seals" TS.

The qualified certificates will be provided by the following certificate authorities (see Annex 4 for detailed information of each certificate authority):
O = Example TSP
Serial = a1 b2 c3 d4

The scope of the conformity assessment is characterized by the service digital identifier (cfr CID (EU) 2015/1505 and ETSI TS 119 612 v2.1.1) of the inspected TS and the following candidate information relevant for inclusion in the national trusted list of the competent supervisory body of the territory in which Example TSP is established.

Qualified certificates for electronic seals will be provided by the following certificate authorities:
O = Example TSP
Service digital identifier = URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Additional service information = http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

The qualified certificates will be provided without the QSCD.

[21] "Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists," Eur-Lex website, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D1505, accessed 24 November 2020.

7. Annex 4 – Audit criteria

7.1 Regulatory

7.1.1 Regulation (EU) No 910/2014 (eIDAS)

The column "articles" indicates which articles of the eIDAS Regulation apply to the QTSP or the specific TS in scope.

QTSP/QTS type	Articles
Qualified trust service provider	5.1, 15, 19.1, 19.2, 23, 24.2 (a) to (j)
Provisioning of qualified certificates for electronic signatures	24.1, 24.2e, 24.2h, 24.2i, 24.2k, 24.3, 24.4, 28.1, 28.3, 28.4, 28.5
Provisioning of qualified certificates for electronic seals	24.1, 24.2e, 24.2h, 24.2i, 24.2k, 24.3, 24.4, 38.1, 38.3, 38.4, 38.5
Provisioning of qualified certificates for website authentication	24.1, 24.2e, 24.2h, 24.2i, 24.2k, 24.3, 24.4, 45.1
Qualified preservation service for qualified electronic signatures	24.2e, 24.2h, 24.2i, 34.1
Qualified preservation service for qualified electronic seals	24.2e, 24.2h, 24.2i, 34.1
Qualified validation service for qualified electronic signatures	24.2e, 24.2h, 24.2i, 32.1, 32.2, 33.1
Qualified validation service for qualified electronic seals	24.2e, 24.2h, 24.2i, 32.1, 32.2, 33.1, 40
Qualified electronic time stamps services	24.2e, 24.2h, 24.2i, 42.1
Qualified electronic registered delivery services	24.2e, 24.2h, 24.2i, 44.1

7.1.2 National requirements

National requirements must be considered based on the country in which the TSP is located. As national requirements are subject to changes, Section 2.2.4 "Regulatory environment" can be seen as an indication of the national regulatory requirements. Proper review of these requirements must be performed during preparation of the conformity assessment and adequate test steps and criteria must be defined to verify the conformity with these additional requirements.

Annex 2 of the certification scheme provides an indicative overview of the national requirements and the impact on the conformity assessment.

7.2 Standards and reference material

QTSP/QTS type	Standards and reference material
Qualified trust service provider	▸ ETSI EN 319 401
Provisioning of qualified certificates for electronic signatures	▸ ETSI EN 319 401 ▸ ETSI EN 319 411-1 ▸ ETSI EN 319 411-2 ▸ ETSI TS 119 412-1 ▸ ETSI EN 319 412-2 ▸ ETSI EN 319 412-5
Provisioning of qualified certificates for electronic seals	▸ ETSI EN 319 401 ▸ ETSI EN 319 411-1 ▸ ETSI EN 319 411-2 ▸ ETSI TS 119 412-1 ▸ ETSI EN 319 412-3 ▸ ETSI EN 319 412-5

QTSP/QTS type	Standards and reference material
Provisioning of qualified certificates for website authentication	▸ ETSI EN 319 401 ▸ ETSI EN 319 411-1 ▸ ETSI EN 319 411-2 ▸ ETSI EN 319 412-4 ▸ ETSI EN 319 412-5
Qualified preservation service for qualified electronic signatures	▸ ETSI EN 319 401 ▸ ETSI TS 119 511 ▸ ANSSI – services de conservation qualifiés des signatures et des cachets électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS – v1.0 du 03 Janvier 2017[22]
Qualified preservation service for qualified electronic seals	▸ ETSI EN 319 401 ▸ ETSI TS 119 511 ▸ ANSSI – services de conservation qualifiés des signatures et des cachets électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS – v1.0 du 03 Janvier 2017
Qualified validation service for qualified electronic signatures	▸ ETSI EN 319 401 ▸ ETSI TS 119 102-1 ▸ ETSI TS 119 441 ▸ ANSSI – services de validation qualifiés des signatures électronique qualifiées et des cachets électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS – v1.0 du 03 Janvier 2017[23]
Qualified validation service for qualified electronic seals	▸ ETSI EN 319 401 ▸ ETSI TS 119 102-1 ▸ ETSI TS 119 441 ▸ ANSSI – services de validation qualifiés des signatures électronique qualifiées et des cachets électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS – v1.0 du 03 Janvier 2017
Qualified electronic time stamp services	▸ ETSI EN 319 401 ▸ ETSI EN 319 421 ▸ ETSI EN 319 422 ▸ ANSSI – services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS – v1.1 du 03 Janvier 2017[24]
Qualified electronic registered delivery services	▸ ETSI EN 319 401 ▸ ETSI TS 119 412-1 ▸ ETSI EN 319 412-2 ▸ ETSI EN 319 412-3 ▸ ETSI EN 319 412-5 ▸ ETSI TS 102 640-3 ▸ ETSI EN 319 521 ▸ ETSI EN 319 531 ▸ ANSSI – services d'envoi recommandé électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS – v1.0 du 03 Janvier 2017[25]

7.3 Versions

Throughout this document, when referring to the above documents, the most current version of the document is referred to.

[22] "Services de conservation qualifiés des signatures et des cachets électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS," *ANSSI website*, https://www.ssi.gouv.fr/uploads/2016/06/eidas_conservation-signatures-cachets-qualifies_v1.0_anssi.pdf, accessed 24 November 2020.

[23] "Services de validation qualifiés des signatures électronique qualifiées et des cachets électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS," *ANSSI website*, https://www.ssi.gouv.fr/uploads/2016/06/eidas_validation-signatures-cachets-qualifies_v1.0_anssi.pdf, accessed 24 November 2020.

[24] "Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS," *ANSSI website*, https://www.ssi.gouv.fr/uploads/2016/06/eidas_horodatage-qualifie_v1.1_anssi.pdf , accessed 24 November 2020.

[25] "Services d'envoi recommandé électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS," *ANSSI website*, https://www.ssi.gouv.fr/uploads/2016/06/eidas_envoi-recommande-electronique-qualifie_v1.0_anssi.pdf, accessed 24 November 2020.

8. Bibliography

The following standards or reference material are referenced by this document:

[1] ISO/IEC 17000:2004, Conformity assessment – *Vocabulary and general principles*

[2] ISO/IEC 17021-1:2015, Conformity assessment – *Requirements for bodies providing audit and certification of management systems - Part 1: Requirements*

[3] ISO/IEC 17065:2012, Conformity assessment – *Requirements for bodies certifying products, processes and services*

[4] ISO/IEC 17067:2013, Conformity assessment – *Fundamentals of product certification and guidelines for product certification schemes*

9. Document history

Version	Date	Description
v0.7	December 2017	Initial draft version
v0.8	December 2017	Structural updates to scheme and resources
v0.9	January 2017	Content updates after review
v1.0	January 2017	Updates based on review and validation of scheme requirements
v1.1	February 2017	Minor structure and reference fixes
v1.2	April 2017	Improved scope definition, indicating regulatory requirements and clarifying test methods

v1.3	September 2019	▸ Updates and revisions to:
		  ▸ Articles
		  ▸ Requirements and scoping of audit criteria
		  ▸ Trust service naming consistency
		  ▸ Transitional arrangements
		  ▸ Surveillance audit criteria
		  ▸ Trusted list definition
		  ▸ Nonconformity timing
		▸ Addition of ETSI EN 319 521, ETSI EN 319 531, ETSI TS 119 495, ETSI TS 119 102-1, TS 119 511, ETSI TS 119 441
		▸ Replacement of ETSI EN 319 412-1 with ETSI TS 119 412-1
		▸ Minor layout changes

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 008839-20Gbl
BMC Agency GA 1017739
ED None

ey.com