EY eIDAS Certification Scheme (accredited scope) for QTSP/QTS conformity assessment against Regulation (EU) 910/2014

EY eIDAS QTSP/QTS certification scheme v1.3

February 7, 2020
Table of contents

1. Introduction ................................................................. 4
  1.1 The eIDAS Regulation on eID and trust services ........................................... 4
  1.2 Accreditation and conformity assessment scheme under eIDAS .................................. 5
2. Certification scheme ........................................................... 8
  2.1 Objectives ........................................................................ 8
  2.2 Scope ............................................................................... 8
    2.2.1 Trust services ....................................................................... 9
    2.2.2 Qualified trust services .......................................................... 9
    2.2.3 Signature and seal creation devices ............................................ 10
    2.2.4 Regulatory environment .......................................................... 10
  2.3 Requirements for conformity assessment body (CAB) .............................................. 11
  2.4 Summary ........................................................................... 12
  2.5 Maintaining the scheme ........................................................................... 13
  2.6 Transitional arrangements ............................................................................ 14
    2.6.1 Transitions between the EY eIDAS certification scheme .................................. 14
    2.6.2 Transition from other schemes .................................................................. 14
  2.7 Contact ............................................................................. 14
  2.8 Resources ........................................................................... 14
3. Certification process ...................................................................... 16
  3.1 Overview ........................................................................... 16
  3.2 Documentation ...................................................................... 17
  3.3 Application .......................................................................... 18
    3.3.1.1 Process overview and activities ......................................................... 18
    3.3.1.2 Review form ............................................................................ 18
  3.4 Application review ......................................................................... 18
    3.4.1.1 Process overview and activities ......................................................... 18
    3.4.1.2 Review the application form ............................................................. 18
    3.4.1.3 Determine audit size ..................................................................... 19
  3.4.2 Preparing the proposal ...................................................................... 19
  3.4.3 Certification efforts ........................................................................ 19
  3.4.4 Certification expenses ........................................................................ 20
3.5 Selection ................................................................................ 21
  3.5.1 Audit criteria ........................................................................ 21
    3.5.1.1 Limited scope certification and assessments ....................................... 21
    3.5.1.2 Standards and reference material ....................................................... 21
    3.5.1.3 Policies .................................................................................. 22
  3.5.2 Preparing the conformity assessment process ................................................ 22
    3.5.2.1 Team selection ........................................................................ 22
    3.5.2.2 Preparing and sending the audit plan ............................................... 22
3.6 Determination .......................................................................... 23
  3.6.1 Overview ........................................................................... 23
  3.6.2 Performing the audit process .................................................................. 23
  3.6.3 Determination activities .................................................................. 24
    3.6.3.1 Definitions ........................................................................... 24
    3.6.3.2 Determination activity type ............................................................ 25
  3.6.4 Documentation request .................................................................. 25
  3.6.5 Stage 1 audit ......................................................................... 26
  3.6.6 Stage 2 audit .......................................................................... 27
  3.6.7 Audit criteria .......................................................................... 29
  3.6.8 Evaluation ............................................................................ 29
    3.6.8.1 Interview ................................................................................ 29
    3.6.8.2 Review of documentation and records ............................................. 29
    3.6.8.3 Observation of processes and activities ........................................... 29
  3.6.9 Sampling methodology ..................................................................... 29
    3.6.9.1 Multi-site sampling .................................................................. 30
3.7 Review .................................................................................................................. 32
  3.7.1 Conformity assessment report ............................................................................ 32
3.8 Decision .................................................................................................................. 33
  3.8.1 Certification decision .......................................................................................... 33
  3.8.2 Certification documentation .............................................................................. 33
3.8.3 Findings ................................................................................................................ 33
  3.8.4 Directory of certified products .......................................................................... 33
3.9 Changes affecting certification ................................................................................ 33
3.10 Conditions on expiration, suspending, withdrawing or reducing scope of certification ... 34
3.11 Attestation .............................................................................................................. 35
  3.11.1 Publication of certificates and use of certification marks .................................... 35
  3.11.2 Complaints and appeals .................................................................................... 35
3.12 Surveillance ............................................................................................................ 36
4. Annex 1 - Qualified trust services defined by the eIDAS Regulation ............................ 37
  4.1 Provisioning of qualified certificates for electronic signatures ............................... 37
  4.2 Provisioning of qualified certificates for electronic seals ....................................... 37
  4.3 Provisioning of qualified certificates for website authentication .......................... 37
  4.4 Qualified preservation service for qualified electronic signatures ......................... 37
  4.5 Qualified preservation service for qualified electronic seals ................................ 38
  4.6 Qualified validation service for qualified electronic signatures .............................. 38
  4.7 Qualified validation service for qualified electronic seals ...................................... 38
  4.8 Qualified electronic time stamps services ............................................................... 38
  4.9 Qualified electronic registered delivery services .................................................... 38
5. Annex 2 - National requirements .............................................................................. 39
  5.1 The Netherlands .................................................................................................... 39
    5.1.1 National implementing law ............................................................................... 39
  5.2 Belgium ................................................................................................................ 40
    5.2.1 National implementing law .............................................................................. 40
6. Annex 3 - Trusted list ............................................................................................... 41
  6.1 Format and specifications ...................................................................................... 41
  6.2 Example contents .................................................................................................. 41
7. Annex 4 - Audit criteria ............................................................................................ 42
  7.1 Regulatory ............................................................................................................. 42
    7.1.1 Regulation (EU) No 910/2014 (eIDAS) ............................................................. 42
    7.1.2 National requirements ...................................................................................... 42
  7.2 Standards and reference material .......................................................................... 43
8. Bibliography ............................................................................................................. 45
9. Document history ..................................................................................................... 46
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, are granted a higher presumption of their legal effect. E.g., 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, fulfilment of the QTSP/QTS requirements and obligations. All those requirements must be met by the QTSP/QTS before providing the very first qualified trust service output, e.g. before issuing the very first qualified time stamp in the case of QTSP providing qualified time stamping services.

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

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

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

\(^1\) See Art.3.16 of the eIDAS Regulation for the definition of trust services.
support provided it meets requirements from Art.23 of the eIDAS Regulation (e.g. a link to the corresponding national trusted list where consumers may verify the granted qualified status must be displayed on the QTSP’s website) and rules of Commission Implementing Regulation (EU) 2015/8062.

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

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

There are nine different types of QTSs 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 services3.

For more information and guidance on the QTSP/QTS initiation process, please refer to ENISA “Guidelines on initiation of qualified trust services”4.

1.2 Accreditation and conformity assessment scheme under eIDAS

The requirements on conformity assessment body (CAB) and the conformity assessment report (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 765/20085, 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 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 QTSP/QTS meet the requirements laid down in the eIDAS Regulation.

---


3 See Annex 1 for more details.

4 https://www.enisa.europa.eu/topics/trust-services/guidelines

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

The eIDAS Regulation does not mandate compliance with any specific standard, and such compliance cannot be made mandatory to TSPs. However, it may be appropriate or even required for the notifying TSP intending to provide QTS to ensure that it complies with specific standards in order to satisfy requirements in another application domain, provided they are not in contradiction with the eIDAS requirements for QTSP/QTS. For example, QTSP providing services for the issuance of qualified certificates for website authentication (QWACs) may be required to meet specific standards to satisfy the CA/Browser Forum 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, so-called the national accreditation body (NAB). All NABs from EU Member States and from 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 ETSI EN 319 403 standard on requirements for CABs to carry out 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 trust service Providers and the trust services they provide towards defined criteria against which they claim conformance.

---

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 SSL/TLS and code signing and has established guidelines to provide greater assurance to Internet users about the web sites they visit by leveraging the capabilities of SSL/TLS certificates. See www.cabforum.org.
It does not, however, specify those criteria nor the certification scheme and needs to be considered as an accreditation “framework” for the conformity assessment of TSP against audit criteria. Those criteria needs 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; and
(iii) be based on standards, publicly available specifications and/or regulatory requirements.

Consequently the EA promoted accreditation scheme (ISO/IEC 17065 completed by ETSI EN 319 403) cannot be implemented unless such effective criteria 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.
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/or 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 as profiled by ETSI EN 319 403 and against the requirements defined in Regulation (EU) No 910/2014 (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, or
   b. the creation, verification and validation of certificates for website authentication; or
   c. the preservation of electronic signatures, seals or certificates related to those services;

II. ‘qualified trust service’ (Art.3.17) means a trust service that meets the applicable requirements laid down in this Regulation;

III. ‘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 non-qualified trust service provider;

IV. ‘qualified trust service provider’ (Art.3.20) means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

V. ‘electronic signature creation device’ (Art.3.22) means configured software or hardware used to create an electronic signature;

VI. ‘qualified electronic signature creation device’ (Art.3.23) means an electronic signature creation device that meets the requirements laid down in Annex II;

VII. ‘electronic seal creation device’ (Art.3.31) means configured software or hardware used to create an electronic seal;

VIII. ‘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;

---

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 Trust Service Providers. This document builds on ISO/IEC 17065 to specify additional requirements for CABs and additional auditing rules under which CABs will have to carry out their conformity assessments of QTSPs and their QTSs. http://www.etsi.org/deliver/etsi_en/319400_319499/319403/02.02.02_60/en_319403v020202p.pdf
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) trust services and (qualified) trust service providers.

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

The present document describes the certification scheme for the issuance of EY CertifyPoint certificates to trust service providers, for the trust services 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 ‘trust services’ by the regulation, we consider the following specific trust services in 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 trust services and trust service providers as qualified trust services (QTS) and qualified trust service providers (QTSP), as the scheme refers to trust services or trust service providers that meet the applicable requirements laid down in the eIDAS Regulation.

Based on the definition of a ‘qualified trust service’ (Art.3.17), a conformity assessment will be performed to assess that a trust service meets the applicable requirements laid down in this Regulation.

Throughout the scheme, we will use the following naming for trust services that meet the applicable requirements in the Regulation. We refer to Annex 1 of this document for the definition of the trust service.

These have been based on guidance documents published by European Union Agency for Network and Information Security (ENISA)\(^\text{10}\) and the related definitions in the ETSI standard\(^\text{11}\) referenced by Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists\(^\text{12}\).

---

\(^{10}\) Guidelines on initiation of qualified trust services v0.7
https://www.enisa.europa.eu/topics/trust-services/guidelines/initiation_tsps

\(^{11}\) ETSI TS 119 612 V2.2.1 (2016-04)
http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.02.01_60/ts_119612v020201p.pdf

\(^{12}\) Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists
2.2.3 Signature and seal creation devices

The certification of qualified electronic signature creation and qualified electronic seal creation devices is out of scope of the scheme. However, during conformity assessment, if applicable according to the trust service(s) 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

2.2.4 Regulatory environment


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 Qualified Trust Services
- 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 recognised 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 member states, member states are free to define implementing laws, defining additional requirements, extending the regulation or for aligning national laws with the regulation.

National requirements must be considered based on the country in which the trust service provider 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 national regulation applicable to an assessment during the preparation phase and define accurate test steps/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)\(^\text{13}\)

\(^\text{13}\) 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) http://wetten.overheid.nl/BWBR0039284/2017-03-10
Annex 2 of the certification scheme provides an indicative overview of national requirements and the impact on 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 conformity assessment of a qualified trust service provider and the qualified trust services 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.

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.
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, efficient to demonstrate QTSP/QTS conformity with all the eIDAS requirements, in such a way that:

► They are organised per type of QTSP/QTS;
► They are organised per requirement of the eIDAS Regulation applicable to a specific type of QTSP/QTS;
► They include sufficient set of criteria to confirm that the assessed QTSP/QTS meets the applicable eIDAS Regulation requirements;
► They ensure that all aspects of the TSP activity are fully covered;
► They take into account the outcome based approach to the eIDAS requirements and not impose specific ways, and in particular no specific standard, for the assessed QTSP/QTS to implement the applicable eIDAS requirements;
► In general, and in particular when based on standards or publicly available specifications:
   ► they are supported by demonstration that the criteria coming from those standards or publicly available specifications are suitable for confirming that the specific applicable eIDAS requirement(s) they support an assessment against are met;
   ► they allow deviation from strict compliance to standards where the requirements from standards 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 <looking for accreditation / accredited> under ISO/IEC 17065, supplemented by ETSI EN 319 403, providing additional dedicated requirements for CABs performing certification of trust service Providers and the trust services they provide towards defined criteria against which they claim conformance.
<table>
<thead>
<tr>
<th>Product / product group that are to be certified</th>
<th>Certification scheme</th>
<th>Standard / normative documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualified trust service provider</td>
<td>EY eIDAS QTSP/QTS certification scheme</td>
<td>Normative: eIDAS Regulation (EU) N°910/2014 including applicable implementing acts and national regulatory requirements</td>
</tr>
<tr>
<td>Trust services (TS) provided by a trust service provider (TSP):</td>
<td>ISO/IEC 17067 scheme type 6</td>
<td>Scheme: EY eIDAS QTSP/QTS certification scheme</td>
</tr>
<tr>
<td>Provisioning of qualified certificates for electronic signatures</td>
<td>Initial review of trust service provider and trust service(s) design</td>
<td>Supporting standards:</td>
</tr>
<tr>
<td>Provisioning of qualified certificates for electronic seals</td>
<td>Initial assessment of trust service provider and trust service(s) implementation</td>
<td>- ETSI EN 319 102</td>
</tr>
<tr>
<td>Provisioning of qualified certificates for website authentication</td>
<td>Initial assessment of trust service provider and trust service(s) operations</td>
<td>- ETSI EN 319 401</td>
</tr>
<tr>
<td>Qualified validation service for qualified electronic signatures</td>
<td>Surveillance:</td>
<td>- ETSI EN 319 411-1 and 411-2</td>
</tr>
<tr>
<td>Qualified validation service for qualified electronic seals</td>
<td>- Assessment of trust service provider and trust service(s) design changes</td>
<td>- ETSI TS 119 412-1 to 412-5</td>
</tr>
<tr>
<td>Qualified preservation service for qualified electronic signatures</td>
<td>- Assessment of the trust service provider and trust service(s)' supporting processes</td>
<td>- ETSI TS 103 171 to 174</td>
</tr>
<tr>
<td>Qualified preservation service for qualified electronic seals</td>
<td>- Assessment of the trust service provider and trust service(s) operations</td>
<td>- ETSI EN 319 421</td>
</tr>
<tr>
<td>Qualified electronic time stamps services</td>
<td></td>
<td>- ETSI EN 319 422</td>
</tr>
<tr>
<td>Qualified electronic registered delivery services</td>
<td></td>
<td>- ETSI TS 102 640-3</td>
</tr>
</tbody>
</table>

### 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 on the domain of trust services 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 national regulation are under development and updates of these requirements are performed on a regular basis.

The certification scheme should be maintained to reflect relevant updates to 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 conformity assessment. As soon as the version is selected, the same version will be used throughout the complete conformity assessment.

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 trust service provider 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 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
E-Mail: 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 filename for each resource.

<table>
<thead>
<tr>
<th>Document(s)</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conformity assessment report</td>
<td>EY eIDAS Conformity Assessment report v6.docx</td>
</tr>
<tr>
<td>Audit plans</td>
<td></td>
</tr>
<tr>
<td>T-15 Audit plan surveillance audit</td>
<td>T-15 Template Audit plan surveillance audit - v0.2_eIDAS.docx</td>
</tr>
<tr>
<td>T-7 Audit plan stage 1 audit</td>
<td>T-7 Template auditplan stage 1 audit - v0.2_eIDAS.docx</td>
</tr>
<tr>
<td>T-8 Audit plan stage 2 audit</td>
<td>T-8 Template auditplan stage 2 audit - v0.2_eIDAS.docx</td>
</tr>
<tr>
<td>Audit reports</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>T-9 Audit report stage 1 audit</td>
<td>T-9 Template audit report stage 1 audit_v0.2_eIDAS.docx</td>
</tr>
<tr>
<td>T-16 Audit report surveillance audit</td>
<td>T-16 Template audit report surveillance audit_v0.2_eIDAS.docx</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application forms</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>F-4</td>
<td>F-4 Application form_v5.6_eIDAS.docx</td>
</tr>
<tr>
<td>F-5a</td>
<td>F-5a Application Review form_eIDAS.docx</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Competence requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>F-11a Competence requirements and qualification procedure for auditors</td>
<td>F-11a Initial evaluation form - Auditor requirements_v2 - Competence requirements and qualification procedure.docx</td>
</tr>
<tr>
<td>F-11b Competence requirements and qualification procedure for audit</td>
<td>F-11b Initial evaluation form - Audit requirements_v2 - Competence requirements and qualification procedure.docx</td>
</tr>
<tr>
<td>F-11c Competence requirements and qualification procedure for eIDAS</td>
<td>F-11c eIDAS requirements evaluation form_v1 - Competence requirements and qualification procedure.docx</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manuals and procedures</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>General Procedures and Processes - ISO 17065 and eIDAS</td>
<td>Quality Manual for ISO 17065 and eIDAS scheme_v1.1.docx</td>
</tr>
<tr>
<td>Quality Manual - eIDAS</td>
<td>Quality procedures for CertifyPoint_v1.1.docx</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work plans</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EY eIDAS Certification Scheme - Requirements mapping guidance</td>
<td>EY eIDAS Certification Scheme - Requirements mapping guidance.docx</td>
</tr>
<tr>
<td>Provisioning of qualified certificates for electronic signature v1.3</td>
<td>Provisioning of qualified certificates for electronic signature v1.3.xlsx</td>
</tr>
<tr>
<td>Provisioning of qualified certificates for electronic seals v1.3</td>
<td>Provisioning of qualified certificates for electronic seals v1.3.xlsx</td>
</tr>
<tr>
<td>Provisioning of qualified certificates for website authentication v1.3</td>
<td>Provisioning of qualified certificates for website authentication v1.3.xlsx</td>
</tr>
<tr>
<td>Qualified preservation service for qualified electronic seals v1.3</td>
<td>Qualified preservation service for qualified electronic seals v1.3.xlsx</td>
</tr>
<tr>
<td>Qualified preservation service for qualified electronic signatures v1.3</td>
<td>Qualified preservation service for qualified electronic signatures v1.3.xlsx</td>
</tr>
<tr>
<td>Qualified validation service for qualified electronic seals v1.3</td>
<td>Qualified validation service for qualified electronic seals v1.3.xlsx</td>
</tr>
<tr>
<td>Qualified validation service for qualified electronic signatures v1.3</td>
<td>Qualified validation service for qualified electronic signatures v1.3.xlsx</td>
</tr>
<tr>
<td>Qualified electronic time stamp service v1.3</td>
<td>Qualified electronic time stamp service v1.3.xlsx</td>
</tr>
<tr>
<td>Qualified electronic registered delivery service v1.3</td>
<td>Qualified electronic registered delivery service v1.3.xlsx</td>
</tr>
</tbody>
</table>
3. **Certification process**

3.1 **Overview**

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

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

   b) Setting-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 to 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 & 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 allow to 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 conformity assessment report containing all the results of the audit will be issued by the CAB to the (Q)TSP. In addition to conformity assessment report, based upon a positive certification decision, a certificate will be issued.

   d) Surveillance assessments and re-certifications: ETSI EN 319 403 under which the certification body of EY CertifyPoint (CAB) has been accredited recommends the CAB to 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 requires in its Art.20.1 QTSPs to “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.

---

Stage 1: obtain and review the documentation on the TSP and the TSP's audited trust service(s)

Stage 2: determine whether the (Q)TSP/(Q)TS is implemented as described in the documentation and complies with the normative requirements

---

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 on the certification process by describing the relevant and public aspects of the process.

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

Several elements of the certification process are supported by internal processes and procedures, who are described in internal process and procedure documentation, 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 against eIDAS regulation, the first action to perform is gathering all required information. For this purpose the process of 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.

3.3.1.1 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 allow to set the timing of the audit, the exact locations where the stages will take place, an assessment/certification proposal regarding the desired area of certification, and on the assessment / certification agreement terms and conditions.

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

3.3.1.2 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(s).

3.4.1.1 Process overview and activities

The process of performing an application review consists of several sub-processes.

3.4.1.2 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:

- 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 trust service(s) 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 competences 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) form.

---

14 Please refer to the documents listed under “Application form” in in section 2.8 “Resources”
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 GTAC assessment or 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.

3.4.1.3 Determine audit size

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

- the size of the trust service scope (e.g. number of information systems used, number of employees, number of certificates issued);
- complexity of the trust service;
- the type(s) of business performed within scope of the trust service;
- extent and diversity of technology utilized in the implementation of the various components of the trust service;
- number of sites;
- previously demonstrated performance of the trust service;
- extent of outsourcing and third party arrangements used within the scope of the trust service;
- the standards, publicly available specifications and regulatory requirements which 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 re-certification audit.

3.4.2 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.\(^\text{15}\)

3.4.3 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 re-certification 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);
- Complexity of the information and communication systems infrastructure (e.g. criticality of information systems, risk situation);
- The component trust services performed;
- Extent and diversity of technology used in the implementation of the various components of the trust services (such as the implemented controls, documentation and/or process control, corrective/preventive action, etc.);
- Number of sites where the trust services are operated/provided;
- In case of surveillance and re-certification audits, the previously demonstrated performance of the TSP/TS;
- 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 PKI processes, Information Security and Service Provider management, in accordance with ETSI EN 319 403.

\(^{15}\) Please refer to the documents listed under “Manuals and procedures” in section 2.8 “Resources”
In general, the initial audit of a TSP/TS whose organization performs all service components for providing a specific trust service would require an effort of <15 to 30> person-days\(^{16}\).

To this should be added 1 person-day for application handling, a maximum of 4 days for preparation, a maximum of 4 person-days for audit reporting (stage 1 audit report, and stage 2 audit report), and 2 person-days for review of audit reports, certification decision and administrative follow-up.

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

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

The above effort estimation are subject to variation in function, notably, of the size and complexity of the TSP organisation and implementation of the trust services it provides that 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.

3.4.4 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.

\(^{16}\) The estimation is based on conformity assessment for one specific trust service
3.5 Selection

3.5.1 Audit criteria

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

- Articles applicable to trust service(s) 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 (ANSSI requirements)

3.5.1.1 Limited scope certification and assessments

Subsets of activities are often outsourced towards other trust service providers, who then perform only a limited set of activities in the context of the trust service (i.e. “component services”).

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

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

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

3.5.1.2 Certification/assessment scope will then be limited to these activities and reporting will clearly indicate the boundaries of the certification/assessment. 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 towards 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 requirements applicable.

3.5.2 Preparing the conformity assessment process
Upon conclusion of the certification contractual agreement, the certification body of EY CertifyPoint will request the TSP makes all necessary arrangements for the conduct of the audit, including provision for examining documentation and the access to all areas, including those of sub-contractors, records (including internal audit reports and reports of independent reviews of information security) and personnel for the purposes of audit, re-certification audit and resolution of complaints.

3.5.2.1 Team selection
The auditors that perform the EY CertifyPoint audits must have the proper technical skillset, 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 offices around the globe.

For each audit, auditors and technical experts will be:

a) selected based on the basis of their competence, training, qualifications and experience; and
b) monitored for the performance during audits.

Requirements towards competences and experience have been defined (forms F-11a, F-11b, F-11c)\(^\text{17}\) 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 competences and experiences.

3.5.2.2 Preparing and sending the audit plan
To ensure 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 on preparing and sending the audit plan to the client.

\(^\text{17}\) Please refer to the documents listed under “Competence requirements” in section 2.8 “Resources”
3.6 Determination

Upon 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 of 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.

![Determination Diagram](image)

**Figure 2**: Overview of the determination activity

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 fulfilment of the specified requirements by the certification object. That includes planning and preparation activities as well as document review, observation and interview.

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

The assessment is organised under a 2-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 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 2 years maximum and depicts the certification mark. A valid certificate authorizes the holder to publicly use the certification mark in connection with the certified qualified trust service 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 TSP’s premises or on any premises used by the TSP to provide its trust services, 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 International Standard, 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); 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 characteristics 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 judgement, 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 Whilst “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 trust service 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 trust services being audited;
- Description of the locations, sizes and functions (tasks and responsibilities) of roles/people involved in the trust services 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;
- Trust service policy (e.g. certificate policy, time stamping policy) and Trust service 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 trust service;
- 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 the interested parties;
  - Description of the risk assessment and treatment methodology;
- Management (in particular Policy Management Authority - PMA) review and meeting minutes;
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 trust service(s). 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 conformity assessment body shall also obtain documentation on the design of the trust service.

The objectives of the stage 1 audit are:

- to audit and review the (Q)TSP/(Q)TS documentation;
- to evaluate (Q)TSP location(s) and site-specific conditions;
- to provide a focus for planning of stage 2 audit by gaining an understanding of the structure and extent of the TSP’s audited trust service(s);
- 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 trust services;
- to collect necessary information regarding the scope of the trust services, processes and location(s) 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, et cetera);
- 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 regards to the preliminary audit of the self-declared partial compliances or non-compliances;

► to evaluate the effectiveness of the trust services management to ensure (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 trust services 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 analyse 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 organisation do not meet the requirements, no onsite 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 its documentation meets the requirements of the applicable normative requirements, the onsite 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 trust services being audited;
► a brief summary of the document review;
► an account of the audit of the information security risk analysis of the TSP's and its trust services being audited;
► a brief assessment of the auditor whether stage 2 is likely to succeed and whether additional resources (e.g. technical experts, more auditors) are required for stage 2;
► audit time spent on document review;
► any areas of concern on whether the TSP's and its trust services being audited meet the requirements of the applicable audit criteria; and
► 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 non-conformity 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 expert of EY CertifyPoint who will decide on the readiness of 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 is implemented as described in the documentation and complies with the normative requirements. The onsite 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; and
  ► to confirm that the implemented trust services 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 evidences on the TSP's trust services with respect to:
- implementation of trust service requirements;
- trust service related organizational processes and procedures;
- trust service related technical processes and procedures;
- implemented information security measures for trust services including IT network protection;
- trust service related products (trustworthy systems) such as cryptographic modules; and
- physical security of the relevant TSP sites.

The onsite 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. Trust service providers' 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 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 trust service provider and the trust service(s) it provides shall take the form of an audit carried out against defined criteria that:

a) take into account specificities of the type of trust service to be assessed;

b) ensure that all aspects of the TSP activity are fully covered; and

c) be based on standards, publicly available specifications and/or regulatory requirements.

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 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 detailed description such as (if applicable): walkthrough of how the control is performed, by who the control is performed, description of the process in which the control is present.

A control that is covered through 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 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 detailed description such as (if applicable): detailed explanation of the control or the process in which the control is present and/or evidence that a control was performed (e.g. based on logs or audit records)

A control that is covered through 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 detailed description such as (if applicable): 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 in 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 e.g. 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, 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 size can be increased.

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

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

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 multiple-site audit based on the following requirements:
- security for all applicable site is administered under control of the organization’s security policy administration; and
- all applicable sites are subject to the organization’s security management review programme.

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 sub-contractor or other external organization;
  - any differing regulatory requirements;
- the sample will be partly selective based on the above in point b) and partly non-selective and result in a range of different sites being selected, without excluding the random element of site selection;
► every site of the organization that is subject to significant threats to assets, vulnerabilities or impacts should be included in the sampling programme;
► the surveillance programme shall be designed in the light of the above requirements and shall, within a reasonable time, cover all sites operations unless it can be demonstrated that this does not impact on the results of the audit; and
► in the case of a nonconformity being observed either at the head office or at a single site, the corrective action procedure shall apply to the head office and to all sites of the operations which may be impacted by the same nonconformity.

The audit shall address the TSP’s central site activities to ensure 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 onsite audit, the auditors prepare a conformity assessment report according to Art.20.1 of the eIDAS Regulation on the basis of the documentary examination and the onsite audit with a statement about the compliance of the trust service 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 fulfils the criteria and is certified conformant;

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 the implementation of corrective actions within 3 months after conclusion of the audit (depending on the type and criticality of the correction(s)); or

c) **not certified**: the audited trust service is not certified conformant.

3.8.2 Certification documentation

At the end of the process, a conformity assessment report containing all 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 2 years maximum and depicts the certification mark. A valid certificate authorises the holder to publicly use the certification mark in connection with the certified qualified trust service according to the EY certification agreement terms and conditions.

3.8.3 Findings

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

Guidance for the classification of findings is as follows:

1. Minor non conformity - 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 trust service provider to achieve its objectives.

2. Major non conformity - an absence of, or the repeated failure to implement and maintain one or more required mandatory standard element, or a situation which would, on the basis of objective evidence, raise significant doubt as to the capability of the trust service provider 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

EYCP will maintain a directory of products that it has certified. It will make the directory publicly accessible with up to date information on certified TSPs and certified trust services they provide.

3.9 Changes affecting certification

There can be instances where certain changes can impact the certification of the organization.

- When the certification scheme introduces new or revised requirements that affect the client, EYCP will ensure these changes are communicated to all clients. EYCP will verify the implementation of the changes by its clients and will take actions required by the scheme.

- Changes affecting certification 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 within certification agreement.

A full re-certification of the TSP’s Trust Services will be performed under the following circumstances:
whenever there are major changes to the scope;
whenever there are major changes to the trust services provided under the scope;
whenever a new trust service is included in the scope;
when there are major changes of IT systems or business processes used by TSP; or
when a major part of the trust services 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 re-certification audit;
► the certified client does not allow surveillance or re-certification 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 transparency of certifications, the certification body maintains a list of the certified products/services which is made available to the public. New certificates are published on the web pages 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/service in publications, catalogues, etc. in compliance with the certification conditions of the certification body of EY CertifyPoint. In case of 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 of 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 procedure is 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 trust service environment and to provide a description of these changes. Based on the severity of these changes, the conformity assessment body must evaluate the need for a surveillance by evaluating the risk of major changes impacting the certification.

2) If initial conformity assessment was performed for one or more new trust service(s) (i.e. the initial conformity assessment was the first conformity assessment for the service(s)), a surveillance audit is recommended to be performed.

3) A surveillance audit must be performed in case exceptions (at least one major or minor non-conformity) are identified during previous conformity assessment.

4) The supervisory body of the applicable member state must be consulted to align on the expectations for performing an intermediate surveillance audit. A surveillance audit must be performed in case of 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 Trust Service Providers that issue Publicly- Trusted Certificates.

A surveillance audit is recommended to 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 interview. The sample is to be designed such that all changes and modifications are covered which have been implemented since the time of the last audit.

The activities to be performed during the different types of audits and assessments are detailed in the applicable audit plans (T-7, T-8, T-15). At maximum one surveillance audit is permitted. After no more than 2 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 trust services listed in Art.3.16 of the eIDAS Regulation for which there are applicable requirements in the Regulation can benefit from the qualified status. eIDAS regulates the following nine qualified trust services:

### 4.1 Provisioning of qualified certificates for electronic signatures

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

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

### 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 an evidence that an electronic data/document was issued by a legal person, ensuring certainty of the data/document’s origin and integrity.

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

### 4.3 Provisioning of qualified certificates for website authentication

Certificates for website authentication are issued to ensure the users (in particular citizens and SMEs) that behind the website there is a legal or natural person identifiable by trustworthy information.

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

### 4.4 Qualified preservation service for qualified electronic signatures

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

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

4.6 Qualified validation service for qualified electronic signatures

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

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

4.7 Qualified validation service for qualified electronic seals

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

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

4.8 Qualified electronic time stamps services

Electronic time stamps are issued to ensure the correctness of the time linked to data/documents.

Qualified electronic time 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 benefit, all over the EU, from the presumption of the integrity of the registered data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by that qualified trust service.

The Regulation sets clear requirements for all such qualified trust services to be considered trustworthy together with obligations for their qualified trust service providers with regard to the security of their operations, their liability and their supervision regime.
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 scope of the scheme (see section 2.2.3 “Signature and seal creation devices”)

\(^{19}\) 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) http://wetten.overheid.nl/BWBR0039284/2017-03-10
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 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
6. Annex 3 - Trusted list

Article 22 of the eIDAS regulation states that “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 Member State. However, as it requires information related to the qualified trust service providers and the related qualified trust services provided by them, within the conformity assessment report, we provide input towards the supervisory body for the trusted list entry.

Section 1.3.2 “Trust service” of the conformity assessment report defines the scope of the conformity assessment and the trust service hierarchy providing this trust service. If applicable, the “service digital identifier”, “additional service information”, “QSCD” and other relevant trust service 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,” 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 been defined as covering “provisioning of qualified certificates for electronic seals” trust service.

The qualified certificates will be provided by the following certificate authorities (see appendix for detailed information of each certificate authority):

O = Example TSP
Serial = a1 b2 c3 d4

The scope of 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 trust service 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
additionalServiceInformation = http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

The qualified certificates will be provided without QSCD

---

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 qualified trust service provider or the specific trust service in scope.

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

7.1.2 National requirements

National requirements must be considered based on the country in which the trust service provider 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/criteria must be defined to verify conformity with these additional requirements.

Annex 2 of the certification scheme provides an indicative overview of national requirements and the impact on conformity assessment.
## 7.2 Standards and reference material

<table>
<thead>
<tr>
<th>QTSP/QTS type</th>
<th>Standards and reference material</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualified trust service provider</td>
<td>► ETSI EN 319 401</td>
</tr>
<tr>
<td>Qualified preservation service for qualified electronic signatures</td>
<td>► 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</td>
</tr>
<tr>
<td>Qualified preservation service for qualified electronic seals</td>
<td>► 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</td>
</tr>
</tbody>
</table>

---

### QTSP/QTS type

<table>
<thead>
<tr>
<th>Qualified validation service for qualified electronic signatures</th>
<th>Standards and reference material</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETSI EN 319 401</td>
<td>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&lt;sup&gt;23&lt;/sup&gt;</td>
</tr>
<tr>
<td>ETSI TS 119 102-1</td>
<td></td>
</tr>
<tr>
<td>ETSI TS 119 441</td>
<td></td>
</tr>
<tr>
<td>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&lt;sup&gt;23&lt;/sup&gt;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Qualified validation service for qualified electronic seals</th>
<th>Standards and reference material</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETSI EN 319 401</td>
<td>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&lt;sup&gt;23&lt;/sup&gt;</td>
</tr>
<tr>
<td>ETSI TS 119 102-1</td>
<td></td>
</tr>
<tr>
<td>ETSI TS 119 441</td>
<td></td>
</tr>
<tr>
<td>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&lt;sup&gt;23&lt;/sup&gt;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Qualified electronic time stamps services</th>
<th>Standards and reference material</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETSI EN 319 401</td>
<td>ANSSI – Services d’horodatage électronique qualifiés - Critères d’évaluation de la conformité au règlement eIDAS - v1.1 du 03 janvier 2017&lt;sup&gt;24&lt;/sup&gt;</td>
</tr>
<tr>
<td>ETSI EN 319 421</td>
<td></td>
</tr>
<tr>
<td>ETSI EN 319 422</td>
<td></td>
</tr>
<tr>
<td>ANSSI – Services d’horodatage électronique qualifiés - Critères d’évaluation de la conformité au règlement eIDAS - v1.1 du 03 janvier 2017&lt;sup&gt;24&lt;/sup&gt;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Qualified electronic registered delivery services</th>
<th>Standards and reference material</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETSI EN 319 401</td>
<td>ANSSI – Services d’envoi recommandé électronique qualifiés - Critères d’évaluation de la conformité au règlement eIDAS - v1.0 du 03 janvier 2017&lt;sup&gt;25&lt;/sup&gt;</td>
</tr>
<tr>
<td>ETSI TS 119 412-1</td>
<td></td>
</tr>
<tr>
<td>ETSI EN 319 412-2</td>
<td></td>
</tr>
<tr>
<td>ETSI EN 319 412-3</td>
<td></td>
</tr>
<tr>
<td>ETSI EN 319 412-5</td>
<td></td>
</tr>
<tr>
<td>ETSI TS 102 640-3</td>
<td></td>
</tr>
<tr>
<td>ETSI EN 319 521</td>
<td></td>
</tr>
<tr>
<td>ETSI EN 319 531</td>
<td></td>
</tr>
<tr>
<td>ANSSI – Services d’envoi recommandé électronique qualifiés - Critères d’évaluation de la conformité au règlement eIDAS - v1.0 du 03 janvier 2017&lt;sup&gt;25&lt;/sup&gt;</td>
<td></td>
</tr>
</tbody>
</table>

### 7.3 Versions

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


Bibliography
The following standards or reference material are referenced by this document.


### 8. Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v0.7</td>
<td>December 2017</td>
<td>Initial draft version</td>
</tr>
<tr>
<td>v0.8</td>
<td>December 2017</td>
<td>Structural updates to scheme and resources</td>
</tr>
<tr>
<td>v0.9</td>
<td>January 2017</td>
<td>Content updates after review</td>
</tr>
<tr>
<td>v1.0</td>
<td>January 2017</td>
<td>Updates based on review and validation of scheme requirements</td>
</tr>
<tr>
<td>v1.1</td>
<td>February 2017</td>
<td>Minor structure and reference fixes</td>
</tr>
<tr>
<td>v1.2</td>
<td>April 2017</td>
<td>Improved scope definition, indicating regulatory requirements and clarifying</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test methods</td>
</tr>
<tr>
<td>v1.3</td>
<td>September 2019</td>
<td>Updates and revisions to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Articles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Requirements and scoping of audit criteria</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Trust service naming consistency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Transitional arrangements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Surveillance audit criteria</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Trusted list definition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Non-conformity timing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Addition of ETSI EN 319 521,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ETSI EN 319 531, ETSI TS 119 495, ETSI TS 119 102-1, TS 119 511, ETSI TS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>119 441</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Replacement of ETSI EN 319 412-1 with ETSI TS 119 412-1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Minor layout changes</td>
</tr>
</tbody>
</table>