Trust Service Provider Conformity Assessment Scheme

Document properties:

Confidentiality Level:	Public
Document Type:	Procedure
Approved by:	DDR

Version history:

Version	Date	Author	Change
0.1	21/12/2016	JAL	Creation
0.2	05/01/2017	OBA	Modification
0.3	06/01/2017	JAL	Modification
1.0	10/11/2017	RSG	Approval
1.1	28/07/2017	JAL	Modification
2.0	28/07/2017	RSG	Approval
2.1	23/09/2017	JAL	Change organization name
3.0	23/09/2017	PDE	Approval
3.1	24/01/2018	JAL	Modification
4.0	24/01/2018	PDE	Approval
4.1	14/02/2018	JAL	Modification
5.0	14/02/2018	RSG	Approval
5.1	01/06/2018	JAL	Modification
6.0	01/06/2018	RSG	Approval
6.1	01/03/2020	RSG	Modification
7.0	08/03/2020	PDW	Approval
7.1	25/06/2020	RSG	Adding all QTSs description
7.2	05/04/2021	RSG	Adding requirements of ETSI 3019 403
8.0	07/04/2021	PDW	Approval
8.1	10/10/2024	KBO	Adding specific requirements for tracing of competence of technical evaluators
9.0	14/10/2024	RSG	Approval
9.1	31/10/2024	JPE	Modification of audit time computation, update of references
10.0	04/11/2024	RSG	Approval
10.1	07/01/2026	PJE	Change in certification decision § 10.5
11.0	09/01/2026	DDR	Approval
11.1	13/03/2026	RSG	Alignment with eIDAS 2
12.0	13/03/2026	DDR	Approval

Table of contents

1 Purpose

This document present the conformity assessment scheme for the purpose of the assessment of the conformity of qualified trust service providers and the qualified trust services. It's included the procedure, the set of rules and the requirements that defines the process requirements for Trust Service Provider Conformity Assessment to ensure that work is completed in a controlled and consistent manner to meet the Article 3.18 of Regulation (EU) 910/2024, amended by 2024/1183 and 2022/2555 and/or the reference standards to comply to requirements of trusted services under Certi-Trust accreditation.

Certi-Trust is accredited to carry out conformity assessment of a QTSP/QTS in accordance with accreditation requirements of ISO 17065, ETSI EN 319 403-1 and ETSI TS 119 403-3.

To date Certi-Trust is not accredited to carry out conformity assessment on those services:

- Qualified electronic attestations of attributes
- Qualified electronic archiving services
- Qualified recording of electronic data in a qualified electronic ledger

2 Scope

This document covers the conformity assessment scheme. It's included assessment processes (planning, execution and reporting) and required procedures listed in article 6.5 of the Commission Implementing Regulation (EU) 2025/2162 for all types of Trust Service Provider Conformity Assessment as listed below:

- Adequacy or Stage 1 assessment
- Registration or Stage 2 assessment
- Follow up assessment
- Surveillance assessment and activities
- Renewal assessment
- Transfer assessment
- Complaint management
- Notifications to the supervisory body
- Competencies of the personnel and auditors

The trust service(s) criteria as defined in ETSI EN 319 403-1 (clause 7.1) can be based on standards, publicly available specifications and/or regulatory requirements. Standards on which criteria for trust service(s) could be based include ETSI standards. Regulatory requirements include
Regulation (EU) 910/2024, amended by 2024/1183 and 2022/2555
and/or national requirements stated by National Control Authority as ANSSI (France), ILNAS (Luxembourg) as example.

As stated in Regulation (EU) 910/2024, amended by 2024/1183 and 2022/2555, Article 20.1:

- Qualified trust service providers shall be assessed at their own expense at least every 24 months by a conformity assessment body.
- The purpose of the assessment 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 and in Article 21 of Directive (EU) 2022/2555.
- 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 conformity assessment body audits the conformity of a trust service provider and the trust service(s) it provides in accordance with the Regulation (EU) 910/2024, amended by 2024/1183 and 2022/2555 (thereafter "eIDAS Regulation") and relevant implementing acts (CID 2015/1405/EU, CID 2015/1406/EU, CID 2016/650/EU, CIR 2015/806/EU). The different types of qualified trust services that are defined in the Regulation (EU) 910/2024, amended by 2024/1183 and 2022/2555 are:

1. Issuance of qualified electronic certificates for eSignatures (QCertForeSig) – Article 28
2. Issuance of qualified electronic certificates for eSeals (QCertForeSeal) – Article 38
3. Issuance of qualified electronic certificates for website authentication (QCertForWSA) – Article 45
4. Issuance of qualified electronic timestamps (QTST) – Article 42
5. Qualified validation of qualified eSignatures (QValForeSig) – Article 33
6. Qualified validation of qualified eSeals (QValForeSeal) – Article 40
7. Qualified preservation of qualified eSignatures (QPresForeSig) – Article 34
8. Qualified preservation of qualified eSeals (QPresForeSeal) – Article 40
9. Qualified electronic registered delivery services (QERDS) – Article 44
10. Qualified service for the management of remote qualified electronic signature creation devices - Article 29a
11. Qualified service for the management of remote qualified electronic seal creation devices - Article 39a
12. Qualified electronic attestations of attributes - Article 45d
13. Qualified electronic archiving services - Article 45j
14. Qualified recording of electronic data in a qualified electronic ledger - Article 45l

In this procedure, TSP standards mean all relevant standards which may be appropriate as guidelines for the assessment. The following standards in annexes of this procedure are expected to be applicable, although this list is not exhaustive. Also, the exact version of a reference standard is confirmed with the assessment plan since new versions are released periodically.

Depending on the country where an eIDAS assessment is performed, specific requirements may be defined by the supervisory body of the country. All specific

requirements by country are defined in annexes and shall be considered. The annexes could be not be exhaustive. It's the responsibility of the TSP to inform Certi-Trust in the application form of all the specific requirements applicable to his service.

Services not defined in eIDAS can be certified and admissible in a trusted list when a national program has been defined. It's the case for the service "Prestataire de Services de Dématérialisation ou de Conservation" of Luxembourg.

Implementing acts have been adopted by the Commission, referencing reference standards the compliance against which leads to the presumption of compliance of QTSP/QTS against the regulatory requirements bearing on them:

- Commission Implementing Regulation (EU) 2025/1567
- Commission Implementing Regulation (EU) 2025/1569
- Commission Implementing Regulation (EU) 2025/1929
- Commission Implementing Regulation (EU) 2025/1942
- Commission Implementing Regulation (EU) 2025/1943
- Commission Implementing Regulation (EU) 2025/1944
- Commission Implementing Regulation (EU) 2025/1946
- Commission Implementing Regulation (EU) 2025/2531
- Commission Implementing Regulation (EU) 2025/2532

Compliance against reference standards is however not mandatory. As such, the demonstration of QTSP/QTS compliance with specific international or European standards differing from the specific documents referenced in the implementing acts can still be used to facilitate demonstrating and certifying QTSP/QTS compliance with the applicable requirements of Regulation (EU) 910/2024, amended by 2024/1183 and 2022/2555. CEN, CENELEC and ETSI have published a wide set of standards with that objective. The annex A provides the list of relevant standards whose compliance is aimed to facilitate demonstration of compliance with requirements from each trusted Services.

A TSP located in a territory outside of Europe can be assess against reference standards and be certified by Certi-trust. However, the assessed trusted services would not be admissible to be qualified and included in the European Trusted List.

3 Normative references

ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

ETSI EN 319 403-1: Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers

ETSI TS 119 403-2: Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies assessing Trust Service Providers that issue Publicly-Trusted Certificates.

ETSI TS 119 403-3: Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers.

ISO/IEC 17065:2012: "Conformity assessment - Requirements for bodies certifying products, processes and services".

ISO/IEC 27006: "Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems".

eIDAS: "REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", amended by 2024/1183 and 2022/2555

NIS2: "DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148" (NIS 2 Directive)

CIR 2024/2690: "Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers"

Note 1: References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.
Definitions and Acronyms

4 Terms and definitions

certification decision: a certification decision, which follows a conformity assessment conducted by a conformity assessment body where that body positively or negatively confirms the conformity of a specific qualified trust service provider and the qualified trust service it provides with the requirements laid down in Regulation (EU) No 910/2014 and with Article 21 of Directive (EU) 2022/2555;

certificate of conformity: a document by which a conformity assessment body attests a certification decision that positively confirms that a specific qualified trust service provider and the qualified trust service it provides comply with the requirements laid down in Regulation (EU) No 910/2014 and with Article 21 of Directive (EU) 2022/2555;

conformity assessment: process demonstrating whether specified requirements relating to a product, process, service, system, person, or body have been fulfilled.

conformity assessment body: body that performs conformity assessment services which is accredited as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides.

conformity assessment report: a document that provides detailed information, where applicable supplementary to that contained in a certification decision and associated certificate of conformity, on the method used to carry out, in accordance with a conformity assessment scheme, a conformity assessment of the compliance of a specific qualified trust service provider and the qualified trust service it provides with the requirements of Regulation (EU) No 910/2014 and of Article 21 of Directive (EU) 2022/2555 and on the results of the conformity assessment;

conformity assessment scheme: a set of rules and procedures to be used by conformity assessment bodies for the purpose of the assessment of the conformity of qualified trust service providers and the qualified trust services that they provide with the requirements laid down in Regulation (EU) No 910/2014 and with Article 21 of Directive (EU) 2022/2555;

national accreditation body: sole body in a State that performs accreditation with authority derived from the State.

qualified trust Service Provider (QTSP): entity which provides one or more qualified electronic trust services.

scheme owner: an entity or a group of entities which is responsible for developing and maintaining a conformity assessment scheme;

trust service: electronic service which enhances trust and confidence in electronic transactions.

trust service component: one part of the overall service of a TSP.

trust Service Provider (TSP): entity which provides one or more electronic trust services.

accreditation: accreditation, as defined in Article 2, point 10 of Regulation (EC) No 765/2008;

flexible scope accreditation: an accreditation where the specific conformity assessment activities for which accreditation is sought, or has been granted, are expressed to allow conformity assessment bodies to make changes in methodology and other parameters which fall within the competence of the conformity assessment body as confirmed by the national accreditation body;

4.1 Acronyms and abbreviations

CA	Certification Authority
CAB	Conformity Assessment Body
EC	European Commission
EU	European Union
IT	Information Technology
TSP	Trust Service Provider

5 Sales

5.1 Client Inquiries for assessment and certification services

In the application form, Certi-Trust needs to ensure to know the list of the trusted service(s) that the TSP applied and need to:

1. consider specificities of the type of trust service to be assessed.

2. ensure that all aspects of the TSP activity are fully covered.

3. and be based on standards, publicly available specifications and/or regulatory requirements. Standards on which those criteria could be based include ETSI EN 319 401 and other standards (ETSI or others). Regulatory requirements on which those criteria could be based include those defined in Regulation (EU) 910/2024, amended by 2024/1183 and 2022/2555 and specific national requirements added. In France, it could be based on the RGS. In all cases, when doing a client inquiry review, a verification of the version of a standard needs to be done.

5.2 Preparation and submission of proposals

When preparing proposals, a site visit and/or a confcall may be necessary to gather more information on the client and to adhere to confidentiality obligations. The scope of the client's trust services activities, the type of solutions used, interfaces with external users and risk assessment results must be taken into consideration. The complexity of the organization will be reflected in an increased or decreased number of days necessary for the assessment.

All increases and decreases from guideline time must be explicitly justified.

5.3 Assessment time determination

Certi-Trust Body shall allow auditors sufficient time to undertake all activities relating to an initial assessment, surveillance assessment and re-assessment. There are no official guidelines or requirements to calculate assessment time determination.

The time allocated shall consider the following factors (following ETSI EN 319 403):

a) the size of the trust service's scope (e.g., number of information systems used, number of employees, number of certificates issued).

b) complexity of the trust service.

c) the type(s) of business performed within scope of the trust service.

d) extent and diversity of technology utilized in the implementation of the various components of the trust service.

e) number of sites.

f) previously demonstrated performance of the trust service.

g) 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 assessment time formula used by Certi-Trust and provided below sets out an average number of assessment days which experience has shown to be appropriate for organizations with a medium number of employees for a single service. A lower number of employees does not decrease nor increase the assessment time due to the fact that operating a trust service with few employees typically leads to higher complexity in ensuring compliance with some requirements, such as access controls requirements, despite decreasing the burden of HR processes. A higher number of employees, however, does lead to a higher assessment time.

NOTE: "Employees" refers to all individuals whose work activities support the scope of certification.

Assessment time for stage 1 solely depends on a complexity factor set by Certi-Trust for the type of trust service to be evaluated.

Assessment time for stage 2 has a non-reducible common basis for all trust services derived from the fact that all trust services have common requirements under the standards declared by Certi-Trust in its conformity assessment scheme as the standards used for assessing the conformity of the trust services to the eIDAS Regulation requirements, to which additional time is added to reflect the additional assessment time required to assess trust service specific requirements. This additional assessment time itself depends on the complexity of the trust service to be assessed and this complexity is categorized into low, medium and high complexity.

Assessment time can be reduced for stage 2 assessment by half a day when the TSP is the holder of an ISO 27001 certification provided this certification explicitly covers in its scope the operations of the trust service to be assessed and provided the certification is no older than 2 years.

The assessment time formula includes on-site assessment time. Time for planning, preparation, interfacing with the client and report writing are included. On-site time does not include travel time. Technical expert is included in the on-site assessment time.

The assessment time formula cannot be used in isolation. The formula identifies a starting point, which should then be adjusted for the specific attributes of the organization and system to be assessed. The number of assessment days must be declined depending on the trust services and the level of complexity.

There shall be a period of no greater than two years for a full (re)assessment unless otherwise required by the applicable legislation or commercial scheme applying.

Surveillance assessments are mandatory in some countries as in Luxembourg. Certi-Trust needs to verify if the supervisory body of the client country requires or not a surveillance assessment. In the absence of requirements, the surveillance assessment is optional.

5.3.1 Assessment time formula

Initial assessment (Stage 1 + Stage 2)

The assessment time formula for initial assessments is:

$$IAT = CS1 + NRBI + CS2$$

Where:

- the non-reducible basis for initial assessments "$NRBI$" is set to be 5 man/days
- the complexity factors $CS1$ and $CS2$ are set according to the two tables below

Complexity factor	Man/days
Low	1.0
Medium	1.5
High	2.0

QTS type	Complexity factor
Issuance of qualified electronic certificates for eSignatures (QCertForeSig)	High
Issuance of qualified electronic certificates for eSeals (QCertForeSeal)	High
Issuance of qualified electronic certificates for website authentication (QCertForWSA)	High
Issuance of qualified electronic timestamps (QTST)	Low

Qualified validation of qualified eSignatures (QValForeSig)	Medium
Qualified validation of qualified eSeals (QValForeSeal)	Medium
Qualified preservation of qualified eSignatures (QPresForeSig)	Medium
Qualified preservation of qualified eSeals (QPresForeSeal)	Medium
Qualified electronic registered delivery services (QERDS)	High
Qualified service for the management of remote qualified electronic signature creation devices	Medium
Qualified service for the management of remote qualified electronic seal creation devices	Medium
Qualified electronic attestations of attributes	High
Qualified electronic archiving services	High
Qualified recording of electronic data in a qualified electronic ledger	Medium

Surveillance assessment

The surveillance assessment time formula is

$$SAT = \frac{1}{3} * IAT + CNC$$

Where:

- the non-reducible basis for surveillance assessments "$NRBS$" is set to be a third of that of the initial assessment time,
- the complexity factor of notified changes CNC is set according to the below table:

Complexity factor	Man/days
Low	0.0
Medium	1.0
High	2.0

Renewal assessment

Renewal assessments required the full re-assessment of the qualified trust service, as such they differ from initial assessments only by the fact that the assessment time might be familiar with the TSP and its services, but it does not reduce the time required to go through the full assessment of each legal and technical requirements.

For this reason, the renewal assessment time is set to be computed as the initial assessment time minus one (1) man/day.

Depending on the trust service provided and their level of complexity of assessment days indicated in the table above must be multiplied by the appropriate factor.

Combined assessments

When there is more than one trust service in scope, the total assessment time is not the sum of all assessment times corresponding to each trust service in scope but, because there are common requirements across all trust services which is accounted for by the non-reducible basis, a modified sum where each additional trust service only adds in the total assessment time its complexity factors plus only half of the non-reducible basis. The assessment time formula for multiple combined assessments when there are N trust services in scope are therefore:

$$IAT = \sum_{i=1}^{N} CS1_i + NRBI * (1 + \left(\frac{N-1}{2}\right)) + \sum_{i=1}^{N} CS2_i$$

For initial assessments and

$$SAT = NRBCS + \sum_{i=1}^{N} \mathrm{CNC_i}$$

For surveillance assessments, where the non-reducible basis for combined surveillance assessments "$NRBCS$" is set to be half of that of the initial assessment time.

For renewal assessments, the reduced time compared to the initial assessment is as man man/days as there are trust services in scope of the assessment.

When the trust services in scope of the combined assessment are similar (e.g. issuance of certificates for electronic signatures and issuance of electronic seals), the complexity factors for all similar trust

services is to be set as "low" except for one of them which remains the same, for the purpose of the computation of the assessment times.

In addition, in case where the trust services in scope of the combined assessment are exceptionally similar, the assessment time can be reduced by $\frac{NRBI}{2}$ days for each additional exceptionally similar trust service.

Trust services that are considered exceptionally similar are:

a) The qualified validation of qualified electronic signature and the qualified validation of qualified electronic seal;
b) The qualified preservation of qualified electronic signature and the qualified preservation of qualified electronic seal.

In addition, the assessment time may be increased or increased depending on other reasons as stated below.

5.3.2 Man-day reduction or increase

Man-days can be reduced for any or all the following reasons:

- Prior knowledge of organization – already registered to another standard
- Client preparedness – already registered with other conformity assessment body
- Maturity of Management System
- Very small site for number of employees
- Single activity process
- High % of employees doing the same low risk tasks
- Combined assessment of an integrated system of two or more compatible management system

Man-days cannot be reduced more than 30% of the assessment calculation time based on the formula.

Man-days can be increased for any or all the following reasons:

- staff speaking more than one language (requiring interpreter(s) or preventing individual auditors from working independently) or documentation provided in more than one language
- Very large site for number of employees
- High degree of regulation
- Complicated logistics involving more than one building or location in the scope of the management system
- System covers high complex processes or relatively high number of unique activities
- Activities that require visiting temporary sites to confirm the activities of the permanent sites(s) whose processes/trust services are subject to certification

- To be defined:
  - High number of employees (more than 25)
  - Complexity of the trusted services
  - Previously demonstrated performance
  - Extent of information system development
  - Number of sites and number of Disaster Recovery (DR) sites
  - Number of registration authorithies
  - For surveillance or renewal assessment: the amount and extent of change relevant

The above lists do not cover all situations and all attributes of the specific organization's processes and products or services should be considered when determining assessment time. In any case, where on-site time deviates from the chart, a record of any additive or subtractive factors shall be made on the Application Approval and Assessment Preparation form.

5.4 Multi-site proposals

5.4.1 Multi-site Certification - Eligibility

The products or services provided by all sites must be substantially of the same kind and must be produced fundamentally according to the same methods and procedures.

The client's information security management system shall be centrally administered under a centrally controlled plan and be subject to central management review. All relevant sites (including the central administration function) shall be subject to the client's internal assessment program and have been assessed in accordance with that program prior to the commencement of an assessment by Certi-Trust.

The central office should also control:

- TSP documentation and system changes
- Complaints
- Evaluation of corrective actions
- Internal assessment planning and evaluation of results

5.4.2 Multi-site Certification - Auditor Days and Sampling

Normally the number of man-days per site should be consistent with the number shown in the Assessment Time Chart above.
The total time expended on initial assessment and surveillance should never be less than that which would have been calculated for the size and complexity of the operation if all the work had been undertaken at a single site.

The following guidance is based on the example of a low to medium risk activity with less than 50 employees at each site. Higher risk activities and larger sites would likely increase the sample size.

Initial Assessment	Central office + square root of number of sites (Including virtual site)
Annual Surveillance Assessment	Central office + 0.6 x square root of number of sites(Including virtual site)
Renewal Assessment	Central office + 0.8 x square root of number of sites (Including virtual site)

This sample can be increased or decreased in respect of factors such as:

- size and number of employees (at one end of the scale a large factory and at the other, non-residential cleaning contracts)
- complexity of the activity
- variation in activities or working practices
- any multinational aspects

When using a sample-based approach, Certi-Trust ensures the following:

a) the initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined.

b) a representative number of sites have been sampled by Certi-Trust, considering:

1) the results of internal assessments of the central site and the other sites.

2) the results of an information security policy management review.

3) variations in the size of the sites.

4) variations in the business purpose of the sites.

5) complexity of the trust service.

6) complexity of the information systems at the different sites.

7) variations in working practices.

8) variations in activities undertaken.

9) potential interaction with critical information systems or information systems processing sensitive information.

10) whether the site is operated by a sub-contractor or other external organization; and

11) any differing regulatory requirements.

c) the sample should be partly selective based on the above in point b) and partly non-selective and should result in a range of different sites being selected, without excluding the random element of site selection.

d) every site of the TSP that is subject to significant threats to assets, vulnerabilities or impacts should be included in the sampling program.

e) the surveillance program shall be designed in the light of the above requirements and shall, within a reasonable time, cover all sites of the TSP operations unless it is demonstrated that this does not impact on the results of the assessment; and

f) 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 TSP operations which may be impacted by the same nonconformity.

The assessment shall address the TSP's central site activities to ensure that central security administration is applied to all sites at the operational level. The assessment should address all the issues outlined above.

Certi-Trust needs to document the justification of the number of sites being subject to the assessment.

5.5 Integrated assessments

For integration with other management system standard(s), application should be made to the relevant Audit Program Manager for that standard in relation to a reduction in assessment time, if applicable.

Man-days cannot be reduced more than 30% of the assessment calculation time based on the formula.

5.6 Extensions, Reductions or Changes to scope

Changes affecting certification initiated by the client may comprise but are not limited to:

a) major changes in the TSP documentation.

b) changes in TSP policies, objectives or procedures affecting the trust service; or

c) security relevant changes.

As required by the Certification Regulation, all changes shall be notified by the client to Certi-Trust. Based on the information provided, appropriate

conformity assessment activities may be done to assess that ongoing conformity is given.

Notification and decision shall be performed before implementation of the measures.

In any cases, there should be a full re-assessment of the TSP's Trust Services under the following circumstances:

a) whenever there are major changes to the scope.

b) whenever there are major changes to the trust services provided under the scope.

c) whenever a new trust service is included in the scope.

d) when there are major changes of IT systems or business processes used by TSP; or

e) when a major part of the trust services moves to another location.

5.7 Transfer of Certification

No special requirements apply.

5.8 Transition assessment

For qualified services whose qualification expires before 20 May 2026, Certi-Trust can do an assessment according to eIDAS 1.0 requirements.

For new applicants and for qualified services whose qualification expires after 20 May 2026, all assessment done by Certi-Trust will be done according to eIDAS 2.0 requirements.

It’s the responsability of the TSP to verify with his supervisory body if specific requirements applied for the renewal of the qualification decision.

Certi-Trust is not accreditated for thoses services

- Qualified service for the management of remote qualified electronic signature creation devices - Article 29a
- Qualified service for the management of remote qualified electronic seal creation devices - Article 39a
- Qualified electronic attestations of attributes - Article 45d
- Qualified electronic archiving services - Article 45j

- Qualified recording of electronic data in a qualified electronic ledger - Article 45l.

An extension request of the accreditation will be done after the transition evaluation from the COFRAC

6 Operations

6.1 Assessment Team Selection

For eIDAS assessment, criteria for the assessment team selection follows rules defined in ISO 27001 Audit Planning, Conducting and Reporting procedure apply.

In each of the following areas at least one auditor in the team shall satisfy auditors' criteria for taking responsibility within the assessment team:

- Managing the team (lead auditor).
- Demonstrated knowledge of the legislative and regulatory requirements and of legal compliance in the field of TSP and information security.
- Demonstrated knowledge of the current technical state-of-art regarding TSP and Public Key Infrastructure.
- Demonstrated knowledge in technologies applicable to the TSP trust service being assessed.
- Demonstrated knowledge of performing information security related risk assessments to identify assets, threats and the vulnerabilities of the TSP and understanding their impact and their mitigation and controls.
- Demonstrated knowledge of organizational reliability issues.

The assessment team should be competent to trace indications of security incidents in the TSP operations back to the appropriate elements of the TSP controls.

Assessment team leaders shall have gained the following experiences and skills in audits under guidance and supervision:

- Having acted as auditor in at least three complete TSP assessments.
- Having adequate knowledge and attributes to manage the assessment process; and
- Having the competence to communicate effectively, both orally and in writing.

The assessment team (which may be an individual) for Stage 2 Assessments shall consist of at least one Lead Auditor and one Auditor with industry qualification.

6.2 Scheduling of assessments

No special requirements apply.

6.3 Scheduling of Surveillance & Renewal Assessments

Surveillance assessments can be conducted periodically.

There shall be a period of no greater than two years for a full (re-) assessment (renewal assessment) unless otherwise required by the applicable legislation or commercial scheme applying the present document.

6.4 Extension to the scope

No special requirements apply.

6.5 Certificate Renewal

No special requirements apply.

6.6 Certification and De-certification database

Certi-Trust also maintains and makes publicly accessible up to date information on certified TSP and certified trust services they provide.

7 Assessment

7.1 General

The objective of the assessment is to confirm and certify that the TSP and the trust services it provides complies with the applicable assessment criteria.

Auditors shall perform their assessment of the TSP and its trust services in at least two stages:

- Stage 1: This stage focuses on obtain and review the documentation on the TSP and the TSP's assessed service(s).
- Stage 2: This stage consists in an on-site assessment that aims to validate the preliminary assessment report findings and to complete the assessment of the TSP assessed services against the assessment criteria. This stage includes:
    - the issuance of an assessment report; and
    - the issuance by the TSP of a Plan of Corrective Actions and its reviewal by Certi-Trust.

7.2 Stage 1 – Planning and Preparation

In preparation for the assessment, auditors shall obtain and review the documentation on the TSP and the TSP's assessed service(s). Auditors shall make the TSP aware of any further types of information and records that may be additionally required for verification during assessment stage 1. In this stage of the assessment, the Conformity Assessment Body shall also obtain documentation on the design of the trust service.

Auditors shall agree, with the TSP, when and where assessment stage 1 is conducted.

7.3 Stage 1 - Assessment

The objectives of assessment stage 1 are to provide a focus for planning of assessment stage 2 by gaining an understanding of the structure and extent of the TSP's assessed service(s).

Assessment stage 1 shall include but shall not be restricted to document review. Other elements that may be included in assessment stage 1 are verification of records regarding legal entity, arrangements to cover liability, contractual relationships between TSP and potential contractors operating or providing sub-component services, internal/external assessments or certifications, security management review, and further investigations with regards to the preliminary assessment of the self-declared partial compliances or non-compliances.

Stage 1 reports shall be submitted by the assessment team leader to Certi-Trust audit program manager. In combination with information held on file, these reports shall at least contain:

a) a 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 assessed.

b) a summary of the document review.

c) a brief description of the trust services component integrated or used in providing the TS separately evaluated, assessed, or certified and their certificates or assessment reports.

d) an account of the assessment of the information security risk analysis of the TSP's and its trust services being assessed.

e) 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.

f) assessment time spent on document review.

g) any areas of concern on whether the TSP's and its trust services being assessed meet the requirements of the applicable assessment criteria; and

h) the assessment methodology employed for stage 1.

In every case, the document review shall be completed prior to the commencement of assessment stage 2.

The results of assessment stage 1 shall be documented in a written report including any recommendations regarding planning for conducting the assessment stage 2. The stage 1 assessment findings, including identification of any areas of concern that could be classified as nonconformity during the stage 2 assessment, shall be communicated to the client.

7.4 Stage 2 – Planning and Preparation

The objectives of assessment stage 2 are:

a) to confirm that the TSP adheres to its own policies, objectives, and procedures; and

b) to confirm that the implemented trust services conform to the requirements of the applicable assessment criteria and abide by the applicable TSP's policies, objectives, and procedures.

In determining the interval between stage 1 and stage 2 assessments, consideration shall be given to the needs of the client to resolve areas of concern identified during the stage 1 assessment. The certification body may also need to revise its arrangements for stage 2.

The assessment team leader shall make the TSP aware of assessment assessment stage 2 planning and of the further types of information and records that may be required for detailed verification during assessment stage 2.

This stage shall always take place at the site(s) of the TSP. Based on observations documented of assessment stage 1, auditors shall draft an assessment plan for the conduct of assessment stage 2.

7.5 Opening Meeting

In addition to the standard opening meeting checklist the following points are checked:

- Confirm that any security clearance requirements of the team have been met and that any declarations have been agreed, e.g., Official Secrets Act.

7.6 Stage 2 - Assessment

During Stage 2 assessment, the assessment shall focus on collecting evidence on the TSP's trust services with respect to:

a) implementation of trust service requirements.

b) trust service-related organizational processes and procedures.

c) trust service-related technical processes and procedures.

d) the trust services components interface. If the trust service uses a trust service component which has already been assessed separately, the trust service assessment team shall check that the requirements of the service component including its security are met, and check that the trust service use of the component interface meets the requirements as specified by the service component provider.

e) implemented information security measures for trust services including IT network protection.

f) trust service-related products (trustworthy systems) such as cryptographic modules; and

g) physical security of the relevant TSP sites.

Evaluation against assessment criteria could include (if applicable for the TSP):

- Pseudonyms in electronic transaction protection (Article 5 of the eIDAS Regulation).
- Provisions concerning liability and burden of proof (Articles 13(1) and 13(2) of the eIDAS Regulation, section 41 of the Identification and Trust Services Act).
- Requirements for accessibility for persons with disabilities (Article 15 of the eIDAS Regulation).
- Security requirements applicable to qualified and non-qualified trust service providers (NIS2 and Article 19a(1) of the eIDAS Regulation); and
- Requirements for qualified trust service providers (Article 24(2) of the eIDAS Regulation excl. Article 24(2)(k)).
- Requirements for qualified certificates (Articles 24(1a)(a)–(d), 24(2)(k), 24(3) and 24(4) of the eIDAS Regulation).
- Requirements for qualified certificates for electronic signatures (Article 28(1) of the eIDAS Regulation).
- Requirements for qualified validation services for qualified electronic signatures (Article 33 of the eIDAS Regulation).
- Requirements for qualified preservation service for qualified electronic signatures (Article 34 of the eIDAS Regulation).
- Requirements for qualified certificates for electronic seals (Article 38 of the eIDAS Regulation).
- Requirements for qualified electronic time stamps (Article 42 of the eIDAS Regulation).
- Requirements for electronic registered delivery services (Article 44 of the eIDAS Regulation).
- Requirements for qualified certificates for website authentication (Article 45 of the eIDAS Regulation).
- Requirements for the qualified service for the management of remote qualified electronic signature creation devices (Article 29a of the eIDAS Regulation).
- Requirements for the qualified service for the management of remote qualified electronic seal creation devices (Article 39a of the eIDAS Regulation).
- Requirements for qualified electronic attestations of attributes (Articles 24(1b)(a)–(e), 24(4a) and 45d of the eIDAS Regulation).

- Requirements for qualified electronic archiving services (Article 45j of the eIDAS Regulation).

- Requirements for Qualified recording of electronic data in a qualified electronic ledger (Article 45l of the eIDAS Regulation).

For organizations that only cover part of activities of a trust service, only applicable criteria shall be assessed. When a requirement is outsourced and/or managed by another entity, assessment team shall ensure that adequate controls are in place (agreement, monitoring process, periodic control process, etc.). Details shall be included in the assessment report.

The TSP assessment report of findings provided by the assessment team leader to Certi-Trust shall be of sufficient detail to facilitate and support a certification decision and shall contain:

a) areas covered by the assessment, including the certification requirements and the sites that were assessed, the significant assessment trails followed, and the assessment methodologies utilized.

b) observations made, both positive and negative.

c) details of any nonconformities identified, supported by objective evidence (if applicable) and a unique reference to the requirement (e.g., ID of the requirement) that is not fulfilled; and

d) comments on the conformity of the TSP and the trust services it provides with the criteria against which the assessment has been carried out, together with a clear statement of nonconformity, and, where applicable, any useful comparison with the results of previous assessments of the TSP and of the concerned trust services.

Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the assessment report as annexes.

Information about the samples evaluated during the assessment should be included in the assessment report, or in other certification documentation.

The report shall consider the adequacy of the internal organization and procedures adopted by the TSP to give confidence in the trust services.

To provide a basis for the decision to confirm that the TSP and its trust services being assessed meet the defined assessment criteria, auditors shall produce clear reports that provide sufficient information to make that decision.

7.7 Closing Meeting

No special requirements apply.

7.8 Assessment report

To support the quality, security and reliability of the qualified trust service provider's activities, the conformity assessment report need to include the minimum information as listed in the annex III of the Commission Implementing Regulation(Eu) 2025/2162.

In particular, for the purpose of facilitating the identification of the service entries to be listed in the national trusted list in accordance with Article 22 of Regulation (EU) No 910/2014, where applicable, a detailed description of the public key infrastructure functional hierarchy, per type of qualified trust service, should be provided in the conformity assessment report.

7.9 Surveillance activites

Surveillance assessments are mandatory in some countries as in Luxembourg. Certi-Trust needs to verify if the supervisory body of the client country oblige or not a surveillance assessment.

By absence of requirements, the surveillance assessment is optional.

Certi-Trust have the rights to perform surveillance activities at any moment, if needed. It can be after receiving a complaint, a request from a supervision body, a verification of the website, etc.

7.10 Surveillance - Assessment

Surveillance assessments need not necessarily be full system assessments. They shall be planned together with other surveillance activities and shall consider a previously applied multisampling strategy.

Each surveillance visit shall include the following items to be assessmented:

- The trusted services maintenance elements such as information security risk assessment and security controls.
- Review of actions taken on nonconformities identified during the previous assessment.
- Review of the multi-site sampling strategy if sampling was applied in the previous assessment.
- Changes to the documented services and TSP operation.
- The functioning of procedures for the periodic evaluation and review of compliance with relevant legislation and regulations.
- Implementation and effectiveness of controls according to the assessment program.

- Treatment of complaints.
- Use of marks and/or any other reference to Certi-Trust.
- Review of any public TSP's statements with respect to its operations (e.g., promotional material, website).

7.11 Renewal Assessment

There shall be a period of no greater than two years for a full (re)assessment unless otherwise required by the applicable legislation or commercial scheme applying the present document.

7.12 Follow-up Assessment

No special requirements apply.

7.13 Special purpose Assessment

The supervisory body may at any time request Certi-Trust to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in the eIDAS Regulation.

7.14 Short notice Assessment

No special requirements apply.

8 Nonconformance and corrective actions.

8.1 General

Each non-conformity must reference the applicable standard clause against which it is raised. Where a significant number of points to watch are raised against any one standard clause then the auditor should give serious consideration to escalating this to a major non-conformity.

To clear any non-conformities raised, both the auditor and the organization's representatives should agree on the necessary corrective action and where appropriate, further actions to prevent recurrence. These actions must be verified by the auditor before clearing the non-conformity.

In situations where the auditor considers that potential non-conformities may arise or where a possible improvement can be identified an observation may be issued. Organizations are free to identify corrective and preventive actions to observations as they wish, but auditors should take note of previous observations raised when performing their assessments and look for signs of improvement.

8.2 Categorization of Nonconformities

8.2.1 Major Nonconformities

No special requirements apply.

8.2.2 Minor Nonconformities

Minor nonconformity shall be understood in eIDAS program as "Points to watch".

8.2.3 Completing and issuing of Nonconformities

No special requirements apply.

8.2.4 Follow up and close out of Major Nonconformities

No special requirements apply.

8.2.5 Follow up and close out of Minor Nonconformities

Minor Nonconformities follow-up and close out shall follow standard process as defined in PRO-7 Audit Planning, Conducting and Reporting. Root cause, curative action and corrective action plan shall be validated by the assessment team.

Corrective actions to address identified Minor Nonconformities shall be documented on an action plan and sent by the organization to the auditor within 30 days for review. If the actions are deemed to be satisfactory, they will be followed up at the next scheduled visit.

The corrective actions for minor non-conformities shall be addressed:

- within 3 months after the notification to the TSP of the assessment report non-conformities; or
- within 6 months after the notification to the TSP of the assessment report non-conformities and it is demonstrated that complexity of the corrective action requires an extended period of time. The TSP shall provide to the assessment team the necessary documentation to evaluate that complexity.

9 Assessment Decision

9.1 General

The assessment decision can be of one of the following three natures:

1. Certified: the assessed trust service fulfils the criteria and is certified conformant.

   Not certified: the assessed trust service is not certified.

2. Not certified before a follow-up assessment: the certification shall not be granted as long as there remain open non-conformities.

9.2 Technical Review and Assessment Decision

Technical review and assessment decision shall be done according to Assessment Report Review Checklist.

9.3 Certificate Preparation and Issue

The certificate (named assessment attestation in ETSI 119 403-3) provide sufficient details to demonstrate that the assessmented TSP fulfilled the requirements of the trusted services. Also, the certificate needs to:

1) be written, at least, in English. If in another language, English will be the official version.

2) be in a "text searchable" PDF format.

3) be uploaded on Certi-Trust's website.

4) Indicate the date on which the assessment decision was made.

5) Indicate the assessment period (dates between assessment evidence have been assessed)

6) Include Certi-Trust name as well as the address, the contact information and information about the applicable accreditation.

7) have an expiry date set to two years after the assessment decision was made.

8) be issued only if no non-conformities are identified

9) shall include a clear identification of the assessed TSP.

10) state the start and end dates of the period that was assessed.

11) state the scope of the certificate.

12) list the assessment standards that were used during the assessment and list the full name and version of the assessment standards referenced.

13) include the identification of the relevant trust service policy (or policies) and/or trust service practices statement(s).

14) include a list of the certificates identifying the service, when appropriate.

Particular attention shall be given to scope statement especially when the organization does not cover all functions and activities of the trust services.

The Certi-Trust certificate for TSPs issuing publicly trusted certificates shall provide sufficient details to demonstrate that the assessed TSP fulfilled the requirements from ETSI EN 319 411-1 and includes the list of the full name, SHA256 thumbprints of the CA certificates of the TSP services that have been assessed, and the applied policies of the assessed TSP.

9.4 Change in certificate

No special requirements apply.

9.5 Publicity of Certification

Certifications are maintained on the Certi-Trust Certified Companies database.

Certi-Trust also maintains and makes accessible up to date information on certified TSP and certified trust services they provide upon request.

9.6 Reference in the Trusted list

A certified provider can be registered in the Trusted List. The Member States of the European Union and European Economic Area publish trusted lists of qualified trust service providers in accordance with the EUDI Framework. The European Commission publishes a list of these trusted lists, the List of Trusted Lists (LOTL). See https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls

The qualified trust service provider is responsible for submitting the resulting conformity assessment report to the supervisory body to be referenced in the Trusted List.

The supervisory body is then responsible for verifying whether the trust service provider and the trust services provided by it comply with the requirements laid down in the eIDAS Regulation, and, with the requirements

for qualified trust service providers and for the qualified trust services they provide.

If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of Article 21.

9.7 Suspension, withdrawal, or cancellation of certification

No special requirements apply.

9.8 Complaint management

No special requirements apply. Certi-Trust ensures that the complaints handling process is publicly available. (*POL-5 available on Certi-Trust website*)

10 Employees Management

10.1 General

Requirements for eIDAS auditors follow the guidelines laid out in ETSI EN 319 403-1 and ETSI TS 119 403-3. When appointing an eIDAS assessment team the attributes below may be divided between the team members.

eIDAS auditors should have the following personal attributes: objective, mature, discerning, analytical, persistent, and realistic. The candidate should be able to put complex operations in a broad perspective and should be able to understand the role of individual units in larger organizations.

10.2 Application reviewer

Certi-Trust personnel in charge of the application form review (Chief Audit Program Officer or the relevant Audit Program Manager) shall have the following specific competences:

- Technological and legal understanding of the areas of activity of the TSP and the associated business risks.

- Technical understanding of the evaluation process.
- Understanding of the competences and capabilities of Certi-Trust.
- Communication and analytic skills to explain certification requirements to the client and to resolve possible difference in understanding regarding standards, other publicly available specifications, or regulatory requirements.

10.3 Auditors

10.3.1 Contract Requirements

No special requirements apply.

10.3.2 Qualification

The criteria for selecting auditors shall ensure that each auditor:

1. Have a formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below.
2. Have at least four years' full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security, and physical security.
3. Has gained experience in auditing information security. This experience should have been gained by participation in a minimum of four audits, including renewal and surveillance audits, for a total of at least 20 days. The participation shall include documentation review, on-site audit, and audit reporting.
4. Have a knowledge of TSP standards and other relevant publicly available specifications.
5. Understand trust services and information security including network security issues.
6. Understand risk assessment and risk management from the business perspective.
7. Have knowledge of security policies and controls.
8. Have successfully completed at least five days of training, the scope of which covers audits and audit management.
9. Have relevant and current experience.
10. Keep current knowledge and skills in information security and auditing up to date through continual professional development.

To have his competencies validated on the RGS assessment in France, an auditor needs to be trained on the specific requirements of ANSSI before performing an assessment mission.

10.3.3 Industry Experience

Auditors involved in auditing shall have knowledge of:

1. the services to be audited.
2. Have general knowledge of regulatory requirements relevant to TSP.
3. industry information security good practices and information security procedures.
4. Policies and business requirements for information security.
5. Information security risks related to business sector.
6. The relevant business sector practices.

10.3.4 Audit Experience

Prior to assuming responsibility for performing as an auditor, the candidate should have gained experience by participation in a minimum of four audits for a total of at least 20 days, including documentation review, on-site audit, and audit reporting. Exceptions may be accepted at the beginning of the program but shall be documented.

Observation stage can be reduced if candidate has award of following professional qualifications:

- Registered national ISMS auditor or lead auditor
- CISSP (Certified Information Systems Security Professional)
- CISA (Certified Information System Auditor)
- CISM (Certified Information Security Manager)
- CIA (Certified Internal Auditor)

Auditors performing as lead auditor should additionally fulfil the following requirements:

- Having acted as auditor in at least three complete audits.
- Having adequate knowledge and attributes to manage the audit process; and
- Having the competence to communicate effectively, both orally and in writing.

Exceptions may be accepted at the beginning of the program but shall be documented.

10.3.5 Demonstration of Competence

As part of the approval process, a Level 1 Audit must be performed by an already approved lead auditor. The Level 1 Audit Report document must be completed as a record of candidate competency. The section "Significant Audit Trails Followed" should explicitly state the following:

- That the candidate has understood the areas of activity of the client organization.

- That the candidate has understood the associated business risks.
- That the candidate has fully understood the information security related threats to assets.
- That the candidate has fully understood the vulnerabilities and impacts of these threats to the client organization.

In addition, for each client organization audited, it must be demonstrated that the auditor is competent for the business area audited.

10.3.6 Additional Skill Qualification

ISO 27001 Audit Planning, Conducting and Reporting shall apply for ISO 27001 audit part (if applicable).

10.3.7 Training

Auditors should have successfully followed a training course on Information Security third party auditing and audit management, in addition to keeping up own knowledge and skill in information security and auditing.

Auditors shall take appropriate training that ensures:

- Knowledge of TSP standards and other relevant publicly available specifications
- TSPs' legal and regulatory requirements.
- Understanding of trust services and information security
- Knowledge of the ISMS standard and other relevant normative documents
- Understanding of risk assessment and risk management from the business perspective
- Technical knowledge of the activity to be audited
- General knowledge of regulatory requirement relevant to TSPs
- Knowledge of security policies and controls
- Knowledge of management systems
- Understanding of the principles of auditing based on ISO 19011
- Knowledge of ISMS effectiveness review and measurement of control effectiveness

10.3.8 Performance Monitoring

No special requirements apply.

10.4 Technical Experts

Where there is a need to supplement Auditor skills with the use of a technical expert, a properly documented agreement covering the arrangements,

including confidentiality and conflict of interests, will be drawn up. Further guidelines can be found in Employees Management procedure.

Technical experts shall also be used for the application review and to qualify the application.

The technical expert must have educated at university level or equivalent (or extensive) professional experience and training which can be equivalent to such a level of education. The technical expert must also have at least three years' full time practical workplace experience in information technology, of which at least two years must be in a role or function relating to information security.

10.5 Certification Manager

Certification decision is taken by the Technical and Quality Director or the Director of the Evaluation Center after a satisfactory review of audit report by a qualified auditor, not being part of the certification process.

Their background and/or experience shall demonstrate their knowledge in:

- standards and publicly available specifications relevant to TSP conformity assessment.
- TSPs general concepts and relevant requirements.
- TSPs' legal and regulatory requirements.
- trust services functioning, and information security management including network security.
- TSPs' security policies and controls; and
- TSPs' risk assessment and risk management.

10.6 Salespeople

Certi-Trust personnel in charge of sales activities shall have knowledge of the program and the specificities:

- Information needed for application.
- Functions and roles of the applicant.
- Context of the application.
- Certification cycle.

10.7 Administrative Personnel

Certi-Trust personnel in charge of administrative activities shall have knowledge of the program and the specificities:

- Information needed for preparing the certificate.
- Information needed for updating the certified company database.

11 Annex 1: List of requirements for type of QTS

11.1 Certification of QTSP under eIDAS regulation

Services	Regulation (EU) No 910/2014
1. **Issuance** of qualified electronic **certificates** for **eSignatures**	Regulation (EU) No 910/2014 of the European Parliament, article: 24(1), 24(2).e, 24(2).h, 24(2).i, 24(2).k, 24(3), 24(4), 28(1) to 28(5), 38(1) to 38(5), 45(1)
2. **Issuance** of qualified electronic **certificates** for **eSeals**	
3. **Issuance** of qualified electronic **certificates** for **website authentication**	
4. **Issuance** of qualified electronic **timestamps**	Regulation (EU) No 910/2014 of the European Parliament, article: 24(1), 24(2).e, 24(2).h, 24(2).i, 24(2).k, 24(3), 24(4), 28(1) to 28(5), 38(1) to 38(5)
5. Qualified **validation** of qualified **eSignatures**	Regulation (EU) No 2024/1183 of the European Parliament, article: 24(2).e, 24(2).h, 24(2).i, 32(1) a to h, 33(1).b, 40
6. Qualified **validation** of qualified **eSeals**	
7. Qualified **preservation** of qualified **eSignatures**	Regulation (EU) No 910/2014 of the European Parliament, article: 24(2).e, 24(2).h, 24(2).i, 34(1), 40
8. Qualified **preservation** of qualified **eSeals**	
9. Qualified electronic **registered delivery** services	Regulation (EU) No 910/2014 of the European Parliament, article: 3(36), 24(2).e, 24(2).h, 24(2).i, 44(1).a to f
10. Qualified service for the management of remote qualified electronic signature creation device	Regulation (EU) No 910/2014 of the European Parliament, article: 24(2).e, 24(2).h, 24(2).i, 29a (1)
11. Qualified service for the management of remote qualified electronic seal creation devices	Regulation (EU) No 910/2014 of the European Parliament, article: 24(2).e, 24(2).h, 24(2).i, 39a
12. Qualified electronic attestations of attributes	Regulation (EU) No 910/2014 of the European Parliament, article: 24(1), 24(2).e, 24(2).h, 24(2).i, 45d(1) to (4)
13. Qualified electronic archiving services	Regulation (EU) No 910/2014 of the European Parliament, article : 24(2).e, 24(2).h, 24(2).i, 45j(1)
14. Qualified recording of electronic data in a qualified electronic ledger	Regulation (EU) No 910/2014 of the European Parliament, article : 24(2).e, 24(2).h, 24(2).i, 45l(1), 45l(2)

11.2 List of standards for type of QTS

For each service, the list of documents is an indication. Other requirements could apply. Documents and applicable versions are available are available on ETSI website: www.etsi.org

11.2.1 Issuance of qualified electronic certificates for eSignatures (QCertForeSig)

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex I to Commission Implementing Regulation (EU) 2025/1943 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
	ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
QTS requirements	ETSI EN 319 412 -1	Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
	ETSI EN 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
	ETSI EN 319 412-5	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
	ETSI TS 119 461	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	CEN EN 419 221-1	Protection profiles for TSP Cryptographic modules – Part 1: Overview
	CEN EN 419 221-2	Protection profiles for TSP Cryptographic modules – Part 2: Protection profile for Cryptographic module for CSP signing operations with backup

	CEN EN 419 221-3	Protection profiles for TSP Cryptographic modules – Part 3: Protection profile for Cryptographic module for CSP key generation services
	CEN EN 419 221-4	Protection profiles for TSP Cryptographic modules – Part 4: Protection profile for Cryptographic module for CSP signing operations
	CEN EN 419 221-5	Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	ISO/IEC 9594-8	Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks
	IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
	IETF RFC 6960	X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

11.2.2 Issuance of qualified electronic certificates for eSeals (QCertForeSeal)

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex II to Commission Implementing Regulation (EU) 2025/1943 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
	ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

QTS requirements	ETSI EN 319 412 -1	Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
	ETSI EN 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
	ETSI EN 319 412-3	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
	ETSI EN 319 412-5	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
	ETSI TS 119 495	Electronic Signatures and Trust Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking
	ETSI TS 119 461	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	CEN EN 419 221 (all parts)	Protection profiles for TSP Cryptographic modules
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	ISO/IEC 9594-8	Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks
	IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
	IETF RFC 6960	X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

11.2.3 Issuance of qualified electronic certificates for website authentication (QCertForeWSA)

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex to Commission Implementing Regulation (EU) 2025/2527 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
	ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
	ETSI TS 119 411-5	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 5: Implementation of qualified certificates for website authentication as in amended Regulation 910/2014
QTS requirements	ETSI EN 319 412 -1	Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
	ETSI EN 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
	ETSI EN 319 412-4	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
	ETSI EN 319 412-5	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
	ETSI TS 119 495	Electronic Signatures and Trust Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking
	ETSI TS 119 461	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	CEN EN 419 221-1	Protection profiles for TSP Cryptographic modules – Part 1: Overview
	CEN EN 419 221-2	Protection profiles for TSP Cryptographic modules – Part 2: Protection profile for Cryptographic module for CSP signing operations with backup

	CEN EN 419 221-3	Protection profiles for TSP Cryptographic modules – Part 3: Protection profile for Cryptographic module for CSP key generation services
	CEN EN 419 221-4	Protection profiles for TSP Cryptographic modules – Part 4: Protection profile for Cryptographic module for CSP signing operations
	CEN EN 419 221-5	Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	CA/Browser Forum BRG	Baseline Requirements Certificate Policy for the Issuance and Management of Publicly Trusted Certificates
	CA/Browser Forum EVG	Guidelines for The Issuance and Management of Extended Validation Certificates
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	ISO/IEC 9594-8	Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks
	IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
	IETF RFC 6960	X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

11.2.4 Issuance of qualified electronic timestamps (QTST)

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex to Commission Implementing Regulation (EU) 2025/1929 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI EN 319 421	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps

QTS requirements	ETSI EN 319 422	Electronic Signatures and Infrastructures (ESI). Time-stamping protocol and time-stamp token profiles
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	CEN EN 419 231	Protection profile for trustworthy systems supporting time stamping
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	IETF RFC 2818	HTTP Over TLS
	IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
	IETF RFC 5816	ESSCertIDV2 update to RFC 3161
	IETF RFC 7230-7235	Hypertext Transfer Protocol -- (HTTP/1.1)
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

11.2.5 Qualified validation of qualified eSignatures (QValForeSig)

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex to Commission Implementing Regulation (EU) 2025/1942 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI TS 119 441	Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services
QTS requirements	ETSI TS 119 442	Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services
	ETSI EN 319 102-1	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
	ETSI TS 119 102-2	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report

	ETSI TS 119 172-4	Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	CEN EN 419 211 (all parts)	Protection Profiles for signature creation & validation application
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ETSI TS 119 101	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation
	ETSI TS 119 612	Electronic Signatures and Infrastructures (ESI); Trusted Lists
	ETSI TS 119 615	Electronic Signatures and Infrastructures (ESI); Trusted Lists. Procedures for using and interpreting European Union Member States national trusted lists
	ETSI TS 119 172-1	Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents
	ETSI EN 319 122 (all parts)	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures
	ETSI EN 319 132 (all parts)	Electronic Signatures and Infrastructures (ESI); XAdES digital Signatures
	ETSI EN 319 142 (all parts)	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures
	ETSI EN 319 162 (all parts)	Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)
	ETSI EN 319 182-1	Electronic Signatures and Infrastructures (ESI); JAdES digital signatures built on JSON Web Signatures
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	IETF RFC 3061	A URN Namespace of Object Identifiers
	IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
	IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
	IETF RFC 5646	Tags for Identifying Languages
	IETF RFC 6960	X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP

	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

11.2.6 Qualified validation of qualified eSeals (QValForeSeal)

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex to Commission Implementing Regulation (EU) 2025/1942 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI TS 119 441	Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services
QTS requirements	ETSI TS 119 442	Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services
	ETSI EN 319 102-1	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
	ETSI TS 119 102-2	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report
	ETSI TS 119 172-4	Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	CEN EN 419 211 (all parts)	Protection Profiles for signature creation & validation application
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ETSI TS 119 101	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation
	ETSI TS 119 612	Electronic Signatures and Infrastructures (ESI); Trusted Lists
	ETSI TS 119 615	Electronic Signatures and Infrastructures (ESI); Trusted Lists. Procedures for using and interpreting European Union Member States national trusted lists

	ETSI TS 119 172-1	Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents
	ETSI EN 319 122 (all parts)	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures
	ETSI EN 319 132 (all parts)	Electronic Signatures and Infrastructures (ESI); XAdES digital Signatures
	ETSI EN 319 142 (all parts)	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures
	ETSI EN 319 162 (all parts)	Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)
	ETSI EN 319 182-1 (draft)	Electronic Signatures and Infrastructures (ESI); JAdES digital signatures built on JSON Web Signatures
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	IETF RFC 3061	A URN Namespace of Object Identifiers
	IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
	IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
	IETF RFC 5646	Tags for Identifying Languages
	IETF RFC 6960	X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

11.2.7 Qualified preservation of qualified eSignatures (QPresForeSig)

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex to Commission Implementing Regulation (EU) 2025/1946 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI TS 119 511 (CONDITIONAL)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
QTS requirements	ETSI TS 119 512	Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services
	ETSI TS 119 172-4	Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	Not applicable	
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ETSI TS 101 533	Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management
	ETSI EN 319 122 (all parts)	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures
	ETSI EN 319 132 (all parts)	Electronic Signatures and Infrastructures (ESI); XAdES digital Signatures
	ETSI EN 319 142 (all parts)	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures

	ETSI EN 319 162 (all parts)	Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)
	ETSI EN 319 182-1	Electronic Signatures and Infrastructures (ESI); JAdES digital signatures built on JSON Web Signatures
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	IETF RFC 3061	A URN Namespace of Object Identifiers
	IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) (TSP)
	IETF RFC 4998	Evidence Record Syntax (ERS)
	IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
	IETF RFC 5646	Tags for Identifying Languages
	IETF RFC 6283	Extensible Markup Language Evidence Record Syntax (XMLERS)
	IETF RFC 6960	X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

11.2.8 Qualified preservation of qualified eSeals (QPresForeSeal)

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex to Commission Implementing Regulation (EU) 2025/1946 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI TS 119 511 (CONDITIONAL)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term

		preservation of digital signatures or general data using digital signature techniques
QTS requirements	ETSI TS 119 512	Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services
	ETSI TS 119 172-4	Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	Not applicable	
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ETSI TS 101 533	Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management
	ETSI EN 319 122 (all parts)	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures
	ETSI EN 319 132 (all parts)	Electronic Signatures and Infrastructures (ESI); XAdES digital Signatures
	ETSI EN 319 142 (all parts)	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures
	ETSI EN 319 162 (all parts)	Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)
	ETSI EN 319 182-1	Electronic Signatures and Infrastructures (ESI); JAdES digital signatures built on JSON Web Signatures
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	IETF RFC 3061	A URN Namespace of Object Identifiers
	IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) (TSP)
	IETF RFC 4998	Evidence Record Syntax (ERS)
	IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
	IETF RFC 5646	Tags for Identifying Languages
	IETF RFC 6283	Extensible Markup Language Evidence Record Syntax (XMLERS)
	IETF RFC 6960	X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

11.2.9 Qualified electronic registered delivery services (QERDS)

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex I and Annex II to Commission Implementing Regulation (EU) 2025/1944 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI EN 319 521 (CONDITIONAL)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
	ETSI EN 319 531 (CONDITIONAL)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers
QTS requirements	ETSI EN 319 522 (all parts) (CONDITIONAL)	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services
	ETSI EN 319 532 (all parts) (CONDITIONAL)	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services
	ETSI TS 119 461	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	Not applicable	
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

Furthermore, auditing this QTS requires knowledge of different authentication assurance frameworks, such as ISO/IEC 29115:2013 "Information technology --

Security techniques – Entity authentication assurance framework" or NIST SP 800-63B "Digital Identity Guidelines Authentication and Lifecycle Management".

11.2.10Qualified service for the management of remote qualified electronic signature creation device

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex to Implementing Regulation (EU) 2025/1567 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI TS 119 431-1	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev
QTS requirements	ETSI TS 119 432	Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation
	CSC API	Cloud Signature Consortium: Architectures and protocols for remote signature applications
	ETSI TS 119 461	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles		
	CEN EN 419 241-2	Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing
	CEN EN 419 221-5	Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	ISO/IEC 9594-8	Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks

11.2.11 Qualified service for the management of remote qualified electronic seal creation devices

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex to Implementing Regulation (EU) 2025/1567 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI TS 119 431-1	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev
QTS requirements	ETSI TS 119 432	Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation
	CSC API	Cloud Signature Consortium: Architectures and protocols for remote signature applications
	ETSI TS 119 461	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	CEN EN 419 241-2	Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing
	CEN EN 419 221-5	Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	ISO/IEC 9594-8	Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks

11.2.12Qualified electronic attestations of attributes

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex I to Commission Implementing Regulation (EU) 2025/1569 may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI TS 119 471	Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services
QTS requirements	ISO 18013-5	Personal identification — ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application
	ISO 18013-7	Personal identification — ISO-compliant driving licence Part 7: Mobile driving licence (mDL) add-on functions
	W3C VC	'Verifiable Credentials Data Model 1.1', W3C Recommendation, 3 March 2022
	ETSI TS 119 461	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	Not applicable	
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ISO/IEC 18013-5	Personal identification — ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application
	FIPS 140-3	Security Requirements for Cryptographic Modules
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

11.2.13Qualified electronic archiving services

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex to Commission Implementing Regulation (EU) 2025/2532may be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
	ETSI TS 119 511 (CONDITIONAL)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
	CEN TS 18170 (CONDITIONAL)	Functional requirements for the electronic archiving services
	ISO 14641 (CONDITIONAL)	Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications
QTS requirements	ETSI TS 119 512	Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services
	ISO 14721	Space Data System Practices — Reference model for an open archival information system (OAIS)
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	Not applicable	
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ETSI TS 101 533	Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management
	ETSI EN 319 122 (all parts)	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures
	ETSI EN 319 132 (all parts)	Electronic Signatures and Infrastructures (ESI); XAdES digital Signatures
	ETSI EN 319 142 (all parts)	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures
	ETSI EN 319 162 (all parts)	Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)
	ETSI EN 319 182-1	Electronic Signatures and Infrastructures (ESI); JAdES digital signatures built on JSON Web Signatures
	ISO/IEC 15408 (parts 1 to 5)	Information technology - Security techniques - Evaluation criteria for IT security

	ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules
	IETF RFC 3061	A URN Namespace of Object Identifiers
	IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) (TSP)
	IETF RFC 4998	Evidence Record Syntax (ERS)
	IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
	IETF RFC 5646	Tags for Identifying Languages
	IETF RFC 6283	Extensible Markup Language Evidence Record Syntax (XMLERS)
	IETF RFC 6960	X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules
	E-ARK CSIP	Common Specification for Information Packages
	E-ARK AIP	Specification for Archival Information
	E-ARK DIP	Specification for Dissemination Information Packages
	ISO 14721	Space data and information transfer systems — Open archival information system (OAIS) — Reference model

11.2.14Qualified recording of electronic data in a qualified electronic ledger

As a general rule, the latest versions of the non-specific references listed below are used.

However, upon explicit request from the TSP, the amended versions referenced in the Annex to Commission Implementing Regulation (EU) 2025/2531 be used.

Constraint	Reference	Name
QTSP requirements	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
QTS requirements	ISO 23257:2022	Blockchain and distributed ledger technologies — Reference architecture
	ISO/TS 23635:2022	Blockchain and distributed ledger technologies — Guidelines for governance
	CEN TS 18170 (CONDITIONAL)	Functional requirements for the electronic archiving services
	ETSI EN 319 122-1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
	ETSI EN 319 132-1	Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures

	ETSI TS 119 182-1	Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures
	ETSI EN 301 549	Accessibility requirements for ICT products and services
Protection Profiles	Not applicable	
Normative references	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	FIPS 140-3	Security Requirements for Cryptographic Modules
	FIPS PUB 140-2	Security Requirements for Cryptographic Modules

12 Annex 2 – Specific requirements in France

Supervisory body in France (ANSSI) has defined specific requirements that shall be considered for all Qualified Trust Service Providers audit for French organization.

Documents and applicable versions are available are available on ANSSI website: https://cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/securite-echanges-voie-electronique/reglement-eidas/referentiels-dexigences/

- Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS
- Services d'horodatage électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS
- Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet - Critères d'évaluation de la conformité au règlement eIDAS
- Services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés - Critères d'évaluation de la conformité au règlement eIDAS
- Services de conservation qualifiés des signatures et des cachets électroniques qualifiés - Critères d'évaluation de la conformité au règlement eIDAS
- Services d'envoi recommandé électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS
- Services d'horodatage électronique qualifiés - Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS
- Services de délivrance des certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet - Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS
- Dispositifs de création de signature / cachet électronique qualifiés - Certification de la conformité au règlement eIDAS

13 Annex 3 – Specific requirements in Luxembourg

Supervisory body in Luxembourg (ILNAS) has defined specific requirements that shall be considered for all Qualified Trust Service Providers audit for Luxembourgish organization:

- ILNAS/PSCQ/Pr001 - Supervision of Qualified Trust Service Providers (QTSPs) (Version 6.6 – 08.07.2024)
- ILNAS/PSCQ/Pr005A – Recognition of other identification methods at the national level (Version 1.5 – 07.05.2024)
- ILNAS/PSCQ/Pr005B - Supplementary Assessment Criteria for Conformity Assessment Bodies for the verification of the requirements in Annex 1 of the procedure ILNAS/PSCQ/Pr005A

Documents and applicable versions are available are available on ILNAS website: www.portail-qualite.public.lu

14 Annex 4 – Specific requirements in Belgium

In Belgium, all eIDAS Services has been adopted in a law (Regulation (EU) 910/2024, amended by 2024/1183 and 2022/2555).

For Electronic archiving services, the applicable standards are listed in an "arrêté Royal" of March 29th, 2019:

- ISO 16175-2:2011
- CoreTrustSeal:2018
- Nestor Seal
- ISO 16363:2012
- ISO 14641:2018
- ISO/TR 13028:2010
- AFNOR NF Z42026:2017

Documents and applicable versions are available are available on SPF Economie website:
https://economie.fgov.be/fr/themes/line/commerce-electronique/signature-electronique-et