Trust Service Provider Conformity Assessment Planning, Conducting and Reporting procedure

Document properties:

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

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

Table of contents

1. Purpose

To meet Article 3.18 of Regulation (EU) No 910/2014 [i.1], Certi-Trust is accredited to carry out conformity assessment of a QTSP/QTS. This procedure defines the process requirements for Trust Service Provider Conformity Assessment to ensure that work is completed in a controlled and consistent manner in accordance with accreditation requirements of ISO 17065 and ETSI 319 403.

2. Scope

This procedure covers audit planning, execution of audit and reporting for all types of Trust Service Provider Conformity Assessment Planning, Conducting and Reporting procedure audits as listed below:

- Adequacy or Stage 1 audit
- Registration or stage 2 audit
- Follow up audit
- Surveillance audit
- Renewal audit
- Transfer audit

The trust service(s) criteria as defined in ETSI 119 403 (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 eIDAS Regulation 910/2014 and/or national requirements stated by National Control Authority as ANSSI (France), ILNAS (Luxembourg) as example.

As stated in eIDAS Regulation 910/2014, Article 20.1:

- Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body.
- The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation.
- The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

The conformity assessment body audits the conformity of a trust service provider and the trust service(s) it provides in accordance with the eIDAS Regulation 910/2014 (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 eIDAS Regulation 910/2014 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

In this procedure, TSP standards mean all relevant standards which may be appropriate as guidelines for the audit. The following standards in annexes of this procedure are expected to be applicable, although this list is not exhaustive.

Depending on the country where eIDAS audit has been done, 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.

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 "Qualified electronic archiving service" of Belgium.

The sole certificate of conformity of a QTSP/QTS against any standard is not sufficient to confirm that QTSP/QTS fulfils the requirements laid down in Regulation (EU) No 910/2014 [i.1] as required by Article 20.1 and Article 21.1 of this Regulation. No secondary legislation has been adopted yet to refer to any standard whose compliance would lead to the presumption of compliance with a sub-set of those requirements. Regulation (EU) No 910/2014 [i.1] does not even foresee such secondary legislation for all the requirements applicable to QTSP/QTSs.

It is however assumed that the demonstration of QTSP/QTS compliance with specific international or European standards will facilitate demonstrating and certifying QTSP/QTS compliance with the applicable requirements of Regulation (EU) No 910/2014 [i.1]. 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.

3. Normative references

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

ETSI TS 119 403-1: 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 auditing 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".

Note: 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.

4. Definitions and Acronyms

4.1. Terms and definitions

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

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

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

4.2. 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 audit 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) No 910/2014. 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. Audit time determination

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

The time allocated shall consider the following factors (following ETSI 419 403):

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.

h) the standards, publicly available specifications and regulatory requirements which apply to the certification.

i) and

j) existing certifications.

The audit time chart of Certi-Trust provided below sets out an average number of audit days which experience has shown to be appropriate for organizations with a given number of employees for a single service. This audit time chart is applicable for TSP issuing qualified certificates for eSignatures with a low complexity. For other services, see the following table with the complexity factor.

"Employees" as referenced in the chart refers to all individuals whose work activities support the scope of certification. The total number of employees for all shifts (including non-permanent or contracted personnel who will be present at the time of the audit) is the starting point for calculating audit time. Part-time employees shall be treated as full-time equivalent employees.

The audit time shown in the chart includes on-site audit 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 audit time.

The audit time chart cannot be used in isolation. The chart identifies a starting point, which should then be adjusted for the specific attributes of the organization and system to be audited. The number of audit 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 audit unless otherwise required by the applicable legislation or commercial scheme applying.

Surveillance audits 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 audit. By absence of requirements, the surveillance audit is optional.

1.1.1. Audit time chart

Initial audit (Stage 1 + Stage 2)

Total Number of Employees	ISO/IEC 27001 certified TSP	Non-ISO/IEC 27001 certified TSP
1 – 10	4,0	6,0
11 – 25	5,5	8,0
26 – 45	6,5	9,5
46 – 65	7,5	11,5
66 – 85	8,5	12,5
86 – 125	9,0	13,5
126 - 175	10,0	15,0
176 - 275	10,5	16,0
276 - 425	11,5	17,0
426 - 625	12,5	18,5
626 - 875	13,5	20,0
876 - 1175	14,0	21,0
1176 - 1550	15,0	22,0
1551 – 2025	16,0	24,0
2026 - 2675	16,5	25,0
2676 - 3450	17,5	26,0
3451 - 4350	18,0	27,0
4351 - 5450	19,0	28,5
5451 - 6800	19,5	29,5
6801 - 8500	20,5	20,5
8501 - 10700	21,0	31,5
>10700	Follow progression above	

Surveillance audit

Total Number of Employees	ISO/IEC 27001 certified TSP	Non-ISO/IEC 27001 certified TSP
1 – 10	1,5	2,0
11 – 25	2,0	3,0
26 – 45	2,5	3,5
46 – 65	3,0	4,0
66 – 85	3,0	4,0
86 – 125	3,0	4,5
126 - 175	3,5	5,0
176 - 275	3,5	5,0
276 - 425	4,0	6,0
426 - 625	4,5	6,5

626 - 875	4,5	7,0
876 - 1175	4,5	7,0
1176 - 1550	5,0	7,5
1551 – 2025	5,5	8,0
2026 - 2675	6,0	8,5
2676 - 3450	6,0	8,5
3451 - 4350	6,0	9,0
4351 - 5450	6,5	9,5
5451 - 6800	6,5	9,5
6801 - 8500	7,0	10,5
8501 - 10700	7,5	11,0
>10700	Follow progression above	

Renewal audit

Total Number of Employees	ISO/IEC 27001 certified TSP	Non-ISO/IEC 27001 certified TSP
1 – 10	3,0	4,0
11 – 25	3,5	5,0
26 – 45	4,5	6,5
46 – 65	5,0	7,5
66 – 85	6,0	8,5
86 – 125	6,0	9,0
126 - 175	6,5	9,5
176 - 275	7,5	11,0
276 - 425	7,5	11,5
426 - 625	8,5	12,5
626 - 875	9,0	13,0
876 - 1175	9,5	14,0
1176 - 1550	10,0	15,0
1551 – 2025	10,5	16,0
2026 - 2675	11,0	16,5
2676 - 3450	12,0	17,5
3451 - 4350	12,0	18,0
4351 - 5450	12,5	18,5
5451 - 6800	13,5	20,0
6801 - 8500	13,5	20,5
8501 - 10700	14,0	21,0
>10700	Follow progression above	

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

When there are more than one services in scope, calculation must be done taking in account the similarity of the requirements. Example: auditing an Issuance of qualified electronic certificates for eSignatures and eSeals will not take twice the time. Adding eSeals in a combined audit will take usually one or two days more depending on the complexity and the numbers of eSeals issued.

Type of QTS	**Complexity**		
	Low	**Medium**	**High**
Issuance of qualified electronic certificates for eSignatures (QCertForeSig)	1.00	1.30	1.60
Issuance of qualified electronic certificates for eSeals (QCertForeSeal)	1.00	1.30	1.60
Issuance of qualified electronic certificates for website authentication (QCertForWSA)	1.00	1.30	1.60
Issuance of qualified electronic timestamps (QTST)	0.75	1.00	1.25
Qualified validation of qualified eSignatures (QValForeSig)	0.85	1.10	1.35
Qualified validation of qualified eSeals (QValForeSeal)	0.85	1.10	1.35
Qualified preservation of qualified eSignatures (QPresForeSig) 1	0.85	1.10	1.35
Qualified preservation of qualified eSeals (QPresForeSeal) 2	0.85	1.10	1.35
Qualified electronic registered delivery services (QERDS)	0.90	1.20	1.50

[1] The coefficient can be further adjusted if the TSP is already certified / compliant with a national legal archiving framework (e.g., PSDC in Luxembourg) and reuses the underlying technology for preserving signatures / seals.

[2] See above note.

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

1.1.2. Man-day reduction or increase

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

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

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

- 0.5 day:
  - 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
- 1 day:
  - 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:
  - Complexity of the trusted services
  - Previously demonstrated performance
  - Extent of information system development
  - Number of sites and number of Disaster Recovery (DR) sites
  - For surveillance or renewal audit: 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 audit 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 Audit Preparation form.

5.4. Multi-site proposals

1.1.3. 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 audit program and have been audited in accordance with that program prior to the commencement of an audit by Certi-Trust.

The central office should also control:

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

1.1.4. Multi-site Certification - Auditor Days and Sampling

Normally the number of man-days per site should be consistent with the number shown in the Audit Time Chart above.
The total time expended on initial audit 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 Audit	Central office + square root of number of sites
Annual Surveillance Audit	Central office + 0.6 x square root of number of sites
Renewal Audit	Central office + 0.8 x square root of number of sites

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

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

5.5. Integrated audits

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 audit time, if applicable.

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.

6. Operations

6.1. Audit Team Selection

For eIDAS audit, criteria for the audit 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 audit 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 audited.
- 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 audit team should be competent to trace indications of security incidents in the TSP operations back to the appropriate elements of the TSP controls.

Audit 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 audits.
- Having adequate knowledge and attributes to manage the audit process; and

- Having the competence to communicate effectively, both orally and in writing.

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

6.2. Scheduling of audits

No special requirements apply.

6.3. Scheduling of Surveillance & Renewal Audits

Surveillance audits can be conducted periodically.

There shall be a period of no greater than two years for a full (re-) assessment audit (renewal audit) 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. Audit

7.1. General

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

Auditors shall perform their audit 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 audited service(s).
- Stage 2: This stage consists in an on-site audit that aims to validate the preliminary audit report findings and to complete the audit of the TSP audited services against the assessment criteria. This stage includes:
    - the issuance of an audit 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 audit, auditors shall obtain and review the documentation on the TSP and the TSP's audited service(s). Auditors shall make the TSP aware of any further types of information and records that may be additionally required for verification during audit stage 1. In this stage of the audit, the Conformity Assessment Body shall also obtain documentation on the design of the trust service.

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

7.3. Stage 1 - Audit

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

Audit stage 1 shall include but shall not be restricted to document review. Other elements that may be included in audit 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 audits or certifications, security management review, and further investigations with regards to the

preliminary audit of the self-declared partial compliances or non-compliances.

Stage 1 reports shall be submitted by the audit 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 audited.

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 audit/assessment reports.

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

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) audit time spent on document review.

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

h) the audit methodology employed for stage 1.

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

The results of audit stage 1 shall be documented in a written report including any recommendations regarding planning

for conducting the audit stage 2. The stage 1 audit findings, including identification of any areas of concern that could

be classified as nonconformity during the stage 2 audit, shall be communicated to the client.

7.4. Stage 2 – Planning and Preparation

The objectives of audit 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 audit criteria and abide by the applicable TSP's policies, objectives, and procedures.

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

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

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

During Stage 2 audit, the audit 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 audited separately, the trust service audit 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 audit criteria could include (if applicable for the TSP):

- Requirements for data processing and 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 trust service providers (Article 19(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 25(1)(a)–(d), 25(2)(k), 25(3) and 25(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); and
- Requirements for qualified certificates for website authentication (Article 45 of the eIDAS Regulation).

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

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

a) areas covered by the audit, including the certification requirements and the sites that were audited, the significant audit trails followed, and the audit 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 audit has been carried out, together with a clear statement of nonconformity, and, where applicable, any useful comparison with the results of previous audits of the TSP and of the concerned trust services.

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

Information about the samples evaluated during the audit should be included in the audit 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 audited meet the defined audit criteria, auditors shall produce clear reports that provide sufficient information to make that decision.

7.7. Closing Meeting

No special requirements apply.

7.8. Surveillance - Planning and Preparation

Surveillance audits 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 audit.

By absence of requirements, the surveillance audit is optional.

7.9. Surveillance - Audit

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

Each surveillance visit shall include the following mandatory items to be audited:

- The trusted services maintenance elements such as information security risk assessment and security controls.
- Review of actions taken on nonconformities identified during the previous audit.
- Review of the multi-site sampling strategy if sampling was applied in the previous audit.
- 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 audit 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).

7.10. Renewal Audit

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

7.11. Follow-up Audit

No special requirements apply.

7.12. Special purpose Audit

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.

7.13. Short notice Audit

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

1.1.5. Major Nonconformities

No special requirements apply.

1.1.6. Points to watch

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

1.1.7. Completing and issuing of Nonconformities

No special requirements apply.

1.1.8. Follow up and close out of Major Nonconformities

No special requirements apply.

1.1.9. Follow up and close out of Points to watch

Points to watch 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 audit team. Implementation of the corrective action will be followed during next audit.

Corrective actions to address identified points to watch 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.

In cases where the follow up evaluation determines that a point to watch identified at a prior visit has not been addressed by the organization, a new, major nonconformity shall be raised if failure and weakness are confirmed.

If a point to watch raised at a prior visit has been addressed but the actions are not complete or have been determined to be ineffective, a new point to watch shall be raised and categorized. The new point to watch statement shall reference the prior point to watch number.

9. Assessment Decision

9.1. General

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

- Conformed: the audited trust service fulfils the criteria and is certified conformant.
- A TSP audit may be passed with pending nonconformities if these do not impact the ability of the TSP to meet the intended service. This assessment decision is conditional upon to the implementation of corrective actions within 3 months after conclusion of the audit for major nonconformities. A follow-up audit is required. For points to watch, correction and corrective action will be reviewed and audit during the next planned audit.
- Not conformed: the audited trust service is not certified.

9.2. Technical Review and Assessment Decision

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

9.3. Certificate Preparation and Issue

The certificate (named audit attestation in ETSI 3019 403-3) provide sufficient details to demonstrate that the audited TSP fulfilled the requirements of the trusted services. Also, the certificate needs to:

1) be written, at least, in English.
2) be in a "text searchable" PDF format.
3) be uploaded on Certi-Trust's website.
4) list the date on which the assessment decision was made.
5) Include Certi-Trust name as well as the address, the contact information and information about the applicable accreditation.
6) be issued annually.
7) be issued only if no critical non-conformities are identified
8) shall include a clear identification of the audited TSP.

9) state the start and end dates of the period that was audited.

10) list the audit standards that were used during the audit and list the full name and version of the audit standards referenced.

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 audited 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 audited, and the applied policies of the audited TSP.

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.

9.4. 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. Suspension, withdrawal, or cancellation of certification

No special requirements apply.

10. Employees Management

10.1. General

Requirements for eIDAS auditors follow the guidelines laid out in ETSI EN 319 403. When appointing an eIDAS audit 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

1.1.10. Contract Requirements

No special requirements apply.

1.1.11. 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 be qualified on the RGS audit in France, an auditor needs to be approved by ANSSI before performing an audit mission.

1.1.12. 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.

1.1.13. 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.

1.1.14. 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.

1.1.15. Additional Skill Qualification

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

1.1.16. 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

1.1.17. 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

Certi-Trust personnel in charge of certification decision (Certification Manager shall have knowledge of:

- 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

10.1 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) à 28(5), 38(1) at 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) à 28(5), 38(1) at 38(5), 45(1)
5. Qualified **validation** of qualified **eSignatures**	Regulation (EU) No 910/2014 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

10.2 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

10.2.1 Issuance of qualified electronic certificates for eSignatures (QCertForeSig)

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 319 412-2	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
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 27001:2013	Information technology — Security techniques — Information security management systems — Requirements
	CA/Browser Forum BRG v1.4.2	Baseline Requirements Certificate Policy for the Issuance and Management of Publicly Trusted Certificates
	CA/Browser Forum EVG v1.6.1	Guidelines for The Issuance and Management of Extended Validation Certificates

	ISO/IEC 15408 (parts 1 to 3)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790:2012	Information technology - Security techniques - Security requirements for cryptographic modules
	ISO/IEC 9594-8:2017	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 (2001)	Security Requirements for Cryptographic Modules

10.2.2 Issuance of qualified electronic certificates for eSeals (QCertForeSeal)

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 319 412-3	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
Protection Profiles	CEN EN 419 221 (all parts)	Protection profiles for TSP Cryptographic modules
Normative references	ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements
	CA/Browser Forum BRG v1.4.2	Baseline Requirements Certificate Policy for the Issuance and Management of Publicly Trusted Certificates
	CA/Browser Forum EVG v1.6.1	Guidelines for The Issuance and Management of Extended Validation Certificates
	ISO/IEC 15408 (parts 1 to 3)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790:2012	Information technology - Security techniques - Security requirements for cryptographic modules

		ISO/IEC 9594-8:2017	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 (2001)	Security Requirements for Cryptographic Modules

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

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 319 412-4	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
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 27001:2013	Information technology — Security techniques — Information security management systems — Requirements
	CA/Browser Forum BRG v1.4.2	Baseline Requirements Certificate Policy for the Issuance and Management of Publicly Trusted Certificates

		CA/Browser Forum EVG v1.6.1	Guidelines for The Issuance and Management of Extended Validation Certificates
		ISO/IEC 15408 (parts 1 to 3)	Information technology - Security techniques - Evaluation criteria for IT security
		ISO/IEC 19790:2012	Information technology - Security techniques - Security requirements for cryptographic modules
		ISO/IEC 9594-8:2017	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 (2001)	Security Requirements for Cryptographic Modules

10.2.4 Issuance of qualified electronic timestamps (QTST)

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
Protection Profiles	CEN EN 419 231	Protection profile for trustworthy systems supporting time stamping
Normative references	ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements
	ISO/IEC 15408 (parts 1 to 3)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790:2012	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 (2001)	Security Requirements for Cryptographic Modules

10.2.5 Qualified validation of qualified eSignatures (QValForeSig)

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 (draft)	Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists
Protection Profiles	CEN EN 419 211 (all parts)	Protection Profiles for signature creation & validation application
Normative references	ISO/IEC 27001:2013	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 v2.1.1	Electronic Signatures and Infrastructures (ESI); Trusted Lists
	ETSI TS 119 615 (draft)	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 3)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790:2012	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 (2001)	Security Requirements for Cryptographic Modules

10.2.6 Qualified validation of qualified eSeals (QValForeSeal)

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 (draft)	Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists
Protection Profiles	CEN EN 419 211 (all parts)	Protection Profiles for signature creation & validation application

Normative references	ISO/IEC 27001:2013	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 v2.1.1	Electronic Signatures and Infrastructures (ESI); Trusted Lists
	ETSI TS 119 615 (draft)	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 3)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790:2012	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 (2001)	Security Requirements for Cryptographic Modules

10.2.7 Qualified preservation of qualified eSignatures (QPresForeSig)

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
Protection Profiles	Not applicable	
Normative references	ISO/IEC 27001:2013	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 (draft)	Electronic Signatures and Infrastructures (ESI); JAdES digital signatures built on JSON Web Signatures
	ISO/IEC 15408 (parts 1 to 3)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790:2012	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 (2001)	Security Requirements for Cryptographic Modules

10.2.8 Qualified preservation of qualified eSeals (QPresForeSeal)

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
Protection Profiles	Not applicable	
Normative references	ISO/IEC 27001:2013	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 (draft)	Electronic Signatures and Infrastructures (ESI); JAdES digital signatures built on JSON Web Signatures
	ISO/IEC 15408 (parts 1 to 3)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790:2012	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 (2001)	Security Requirements for Cryptographic Modules

10.2.9 Qualified electronic registered delivery services (QERDS)

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
Protection Profiles	Not applicable	
Normative references	ISO/IEC 27001:2013	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 3)	Information technology - Security techniques - Evaluation criteria for IT security
	ISO/IEC 19790:2012	Information technology - Security techniques - Security requirements for cryptographic modules
	FIPS PUB 140-2 (2001)	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".

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: www.ssi.gouv.fr

- Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS (Version 1.2 du 05 juillet 2017)
- Services d'horodatage électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS (Version 1.1 du 3 janvier 2017)
- 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 (Version 1.1 du 3 janvier 2017)
- Services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés - Critères d'évaluation de la conformité au règlement eIDAS (Version 1.0 du 3 janvier 2017)
- Services de conservation qualifiés des signatures et des cachets électroniques qualifiés - Critères d'évaluation de la conformité au règlement eIDAS (Version 1.0 du 3 janvier 2017)
- Services d'envoi recommandé électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS (Version 1.0 du 3 janvier 2017)
- Services d'horodatage électronique qualifiés - Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS (Version 1.1 du 3 janvier 2017)
- 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 (Version 1.1 du 3 janvier 2017)
- Dispositifs de création de signature / cachet électronique qualifiés - Certification de la conformité au règlement eIDAS (Version 1.0 du 16 novembre 2017)

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 6.1 – 12.12.2019)
- ILNAS/PSCQ/Pr005 - ILNAS/PSCQ/Pr001 - Supervision of Qualified Trust Service Providers (QTSPs) (Version 1.2 - 12.12.2019)

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 (Law of July 21, 2016). Supervisory body in Belgium (SPF Economie – Service Public Fédéral Économie) has defined one other specific service, Qualified Electronic Archiving.

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