F-2319

CERTIFICATION REQUIREMENTS OF TRUST SERVICE PROVIDERS (TSP)

Number: F-2319
Issue Date: 2017-04-06
Revision No: 5
Revision Date: 2024-04-02

Q-CERT

Contents

1. Introduction

1.1. Scope

This document describes QMSCERT's regulation for the assessment of Trust Service Providers (TSPs) and the services which they provide against the applicable requirements which fall under Reg. EU 2014_910 "eIDAS" and the ETSI EN 319 403-1 accreditation scheme, including technical specifications ETSI TS 119 403-2 and ETSI TS 119 403-3, where applicable.

The objective of QMSCERT is to verify compliance with the applicable requirements, deriving from the eIDAS Regulation, the ISO / IEC 27001 standards (where applicable) and the supporting ETSI standards (See section 1.3 "*Standards*"). The evaluation considers also any additional documents indicated by the Competent Supervisory Body, and the effective continuous operation of the services subject to certification, including reliability and effective and tested predispositions of business continuity and recovery from catastrophic damage situations (so-called Disaster Recovery).

QMSCERT evaluates through the audits conducted and the analysis of the reports, whether the infrastructure and the services provided are intrinsically secure, designed with criteria oriented towards information security and cybersecurity and that trust services are provided through infrastructures whose physical, logical and organizational elements are such as to allow the highest level of resilience and ability to respond to possible threats, both internal and external.

QMSCERT's assessment covers the services that the TSP has declared to the Supervisory Body with particular focus on the effectiveness, reliability and resilience to threats of the same, and also with reference to any outsourced processes to third parties.

1.2. Background

This Certification Regulation has been prepared in order to give clear indications to the Trust Service Providers (TSPs) of the requirements to be followed for the purpose of requesting and maintaining certification in the eIDAS scheme, and to provide clear regulatory indications on the responsibilities and expectations towards them.

eIDAS trust services are a substantial element to support market development in the EU and in the countries that intend to be our partners, therefore, the trust services defined by the eIDAS Regulation, as well as national ones, are considered strategic for the economic and social development of the EU itself and the domestic market.

To this end, the physical, logical and organisational infrastructures supporting eIDAS trust services, as certified, must guarantee not only the existence and effectiveness of such trust services, but above all their reliability in terms of business continuity, market response capacity and maximum resilience against possible internal and external threats and dangers, both aimed at the infrastructures themselves, and aimed at the dimensions of cyberspace in which the related trust services are provided.

1.3. Standards

The relevant ETSI standards are:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-4: Certificate Profiles; Part 4: Certificate profile for web site certificates
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles
- ETSI TS 119 511: Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- ETSI EN 319 521: Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI EN 319 531: Policy and security requirements for Registered Electronic Mail Service Providers
- ETSI EN 319 522xx: Electronic Registered Delivery Services
- ETSI EN 319 532xx: Registered Electronic Mail (REM) Services
- ETSI TS 119 441: Policy requirements for TSP providing signature validation services
- ETSI EN 319 102-1: Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI TS 119 612: Trusted Lists
- ETSI TS 119 615: Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists
- ETSI TS 119 461: Policy and security requirements for trust service components providing identity proofing of trust service subjects

For certificate issuance services which relate to international schemes (e.g. Publicly Trusted Certificates, such as TLS, Code-Signing, Email Protection) the relevant requirements (e.g. CA/B Forum: Baseline Requirements, Extended Validation Guidelines for Server Authentication Certificates, Code Signing Requirements) also apply.

The above standards are intended to apply to the TSPs in accordance with the services they provide. As a general rule, the latest available version of the standards is used, taking into account the time reasonably required for their implementation.

This regulation and all related documentation are subject to evaluations from designated staff of the Accreditation Body; Supervisory Body (EETT for Greece, AgID for Italy and so on) designated staff may also be present during these evaluations.

2. Certification requirements

2.1. General requirements

General requirements for the TSP:

1) Where required by the regulations, standards and technical specifications, there will be documented procedures.
2) Completion and record of at least one full internal audit cycle for all applicable requirements of the related standards (when applicable).
3) Records that prove the application and implementation of the related standards (when applicable).
4) Completion and documentation of at least one management review which includes an assessment of the systems continuing suitability, adequacy and effectiveness and opportunities for improvement of the related standards (when applicable).
5) Objective evidence that the Trust Services provisioning processes are monitored and measured in relation to objectives for security and compliance.
6) In the case of TSPs with at least one site in Italy, certification against ISO/IEC 27001, covering the trust services in question, is mandatory as established by the Italian Supervisory Body (AgID).
7) The TSP accepts the presence of Inspectors from the Accreditation Body during the different audit phases carried out by QMSCERT's audit team. Failure to accept this requirement prevents any activity inherent in the eIDAS scheme from continuing.
8) In addition, the TSP accepts that both the Accreditation Body and the competent Supervisory Body are able to intervene at all stages and at all sites and working environments, as observers, during compliance audits applicable to the scheme.

2.2. Risk assessments

QMSCERT evaluates the risk analysis of the TSP for its services, at least for the following aspects:

1) an internal and external scenario analysis, with particular reference to the elements referable to the attack surfaces or that can interact with them. To complete this analysis on the external and internal context, a "SWOT" analysis must be prepared, with the related assessments for the management of weaknesses and threats;
    a) the external scenario analysis must contain at least the assessment of the dynamics of the threats that may have an impact on the TSP;

b) the internal scenario analysis must contain at least the assessment of the status of the VA and the results of the PTs, their completeness with respect to the attack surfaces and the actions planned for their management;

2) the assessment of the updating of the skills and methods adopted by the TSP Management to create awareness among the Human Resources of the organization in the face of security needs;
3) the assessment of the formal acceptance of the residual risk by the management of the TSP itself;
4) the assessment of the adoption by the TSP of "best practices" for carrying out risk assessment such as the ISO 27005 standards and, at systemic level, the ISO 31000;
5) the assessment of critical issues related to interfaces and dependencies with other IT infrastructure services – scenario analysis and changes to the ICT infrastructure – relationship with 27001);
6) the assessment of the correct management of the credentials for accessing the systems;
7) the assessment of the ability to manage incidents, their recognition and registration (ticketing) and their management, in particular in the case of potential "Data Breaches", with reference to the procedure for their management;
8) the evaluation of the definition of the SW development cycle, change management (including SW), separation from test and production environments;
9) the assessment of the correct mapping of the TSP assets,
10) the evaluation of the adoption of a procedure for communication, which takes into account emergency situations, such as so-called "data breaches";
11) the evaluation of exercises to verify the effectiveness of solutions for business continuity and system recovery after catastrophic events.

QMSCERT evaluates that the results of the risk assessment find an appropriate and timely response commensurate with the level of the criticalities highlighted.

2.3. Internal audits

QMSCERT evaluates the internal audits of the TSP for its services, at least for the following aspects:

1) the correct application of the classification of the findings found during the Internal Audit activities;
2) the qualification of Internal Auditors and their maintenance;
3) the guarantee of independence of the Internal Auditors, with respect to the processes evaluated;
4) the planning of the Internal Audit cycle at least every two years, developed on the basis of the evidence emerging from the risk assessment of the TSP processes, therefore based on the need to test the operational controls carried out to mitigate these risks. The planning must take into account the results of the Internal Audits of the last two years, the need to monitor the effectiveness of previous corrective actions and the similar outcome of the management of the external audit results and supervision by the competent SB;

5) the sampling criteria of critical processes, taking into account the number of these entities, or by grouping into clusters defined on the basis of specific criteria (e.g. management of remote signature QSCD for a specific customer), considering the criteria of the UNI 2859 standard;
6) with reference to the identification processes, tests carried out with mystery auditing techniques and subsequent reconstruction tests of the identification processes must be provided, to guarantee the complete reliability of this process, bearing in mind that it is the process with the highest level of risk and importance managed by the TSPs themselves. In the event that incognito audit is not feasible (e.g. if signature services are provided only to employees, or members of trade associations), the QTSP must demonstrate that it has carried out ex post reconstruction tests of the identification processes, the entrustment to third parties of critical processes or that may represent critical issues for information security and cybersecurity, in particular where the security of users' personal information is concerned – for various reasons – of the TSP services.

2.4. Robustness of IT Systems

QMSCERT verifies the existence and acceptability of the VA (Vulnerability Assessment) and PT (Penetration Test) services, ensuring that they are extended to a security perimeter, which allows to guarantee resilience on the entire physical, logical and organizational infrastructure, however correlated with the services for which certification is required.

1) It is not sufficient to carry out a VA-PT on the surface represented by the exposure of only the hardware, software and physical places through which the services subject to certification are offered, but that interfaces to other parts of the connected infrastructure must also be included, to the extend they participate in the provision of the services subject to certification.
2) The documented analysis on the need for VA-PT must take into account all possible attack surfaces, including interfaces with the sections of the TSP infrastructure assigned to other services, TCP/IP layer management, APIs, internal and external libraries, SWs, in particular the so-called "open source", cloud environments etc.
3) For TSPs with at least one location in Italy, the laboratories in charge of operational controls relating to VA processes must be accredited according to ISO/IEC 17025. For TSPs with offices in other EU countries, VAPT tests must be carried out with accredited laboratories where available, or by suppliers who provide at least the following evidence:
   a) the clear identification and diligent application of the requirements inherent in the technical assessment methodology adopted, which refers, preferably, to the application of the ISO/IEC 27008 requirements;
   b) the guarantee of the specific formal competence (such as qualifications, from whom you issue, what experience in the sector) of the Human Resources involved in these tests;
   c) the qualification (certification in IT jargon) of the SW used (at least the guarantee that the versions are compatible and updated to the releases of the OS and applications to be analyzed of the TSP that performs conservation services), as well as constantly updated with reference to the official databases on known vulnerabilities (eg databases for each configuration element, edited by national CSIRTs or other qualified sources such as MITRE (https://cve.mitre.org/cve/).

4) The evaluation and qualification of the LAB/suppliers is always the responsibility of the TSP.
5) The evidence of this qualification process is assessed as part of the audit process by QMSCERT.
6) If the TSP has delegated the identification of the VA-PT Laboratory to QMSCERT, the criteria adopted by QMSCERT will be examined during verification by the Accreditation Body.
7) QMSCERT shall ask whether a formal process and/or a documented procedure is adopted for the management of the VA/PT process and evaluate its effectiveness in terms of:
   a) verification of the understanding of the laboratory evaluation report by formal act;
   b) assessment of the impact of the vulnerabilities found in the report in relation to remediation times;
   c) definition of a plan for correcting the results, depending on the level of criticality, as described in the LAB report.
8) QMSCERT ensures that the results of the safety analyses (VA tests and PT tests) find an immediate response commensurate with the level of the criticalities highlighted.
9) The SB will take into account the rationale adopted by the TSP in the planning of vulnerability resolution in the face of the critical issues encountered, with reference to the needs of robustness and resilience of the infrastructure and existing insurance coverage.
10) In the event that the vulnerabilities found and classified as critical are not promptly removed and / or the correction plan is not implemented on time, thus determining a potential vulnerability for information security, which may compromise or may have compromised the services, QMSCERT issues a NC.
11) Further, referring both to the management of the deficiencies found and to the inadequate commitment (commitment) of the Management. At the same time, QMSCERT shall initiate the process of suspension of the TSP, which – in the absence of timely correction actions – must be completed no later than one month from the opening of the same major NC.

2.5. Outsourcing

The following apply for TSPs with essential processes outsourced or fully outsourced services managed in conformity with the eIDAS Regulation:

1) The TSP/QTSP shall maintain an up-to-date list of third parties to whom it has delegated all or part of its processes, with particular reference (specific section of the list) to processes that directly impact eIDAS services. These processes will have to be mapped, the description of how the "outsourcer" governs them, the methods adopted for monitoring, including the right to auditing without restrictions.
2) In cases of a QTSP which allocates one or more HSMs/QSCDs to one or more customers under its responsibility, the QTSP shall ensure adequate operational monitoring and control criteria of these devices, ensuring the right to perform audits and access authorization for QMSCERT's auditors and inspectors/observers of the Accreditation Body and/or the Supervisory Body.
3) QMSCERT shall carry out evaluations at these operators taking into account the fact that the essential processes for services in accordance with the eIDAS Regulation (not support processes) shall be performed by QTSPs. Support process is meant any process which does not have a direct impact on the service provided in accordance with the eIDAS Regulation.

4) In general, QMSCERT evaluates how the TSP manages third parties starting from the most critical activities, such as the Registration Authorities (RA), for which evidence of control must be given through shared and contractually signed sub-process assignment procedures that provide for at least the possibility of conducting audits (even incognito - internal mystery auditors), the commitment to the management and communication of incidents also in the face of applicable legislation (eg: data breach ex GDPR), management of shared KPIs).
5) In assessing the services of TSPs that have been allocated outside, in "outsourcing" mode, the Certification Authority must verify that these "outsource" providers are qualified as QTSP (qualification obtained against the "eIDAS" Regulation).
6) In such cases of outsourced processes at other QTSPs, the evaluation shall be performed only against ETSI EN 319 401, and the modalities adopted to ensure the control of outsourced processes. This also applies to the delivery of QTSP processes in "full outsourcing" mode (i.e. “Managed PKI”).
7) Outsourcing of essential services (e.g. HSM/QSCD management, management of CRL databases, management of Registration Authorities) to unqualified operators (non-QTSP) is not permitted. In any case, where this is not possible, the TSP must give evidence that these suppliers are evaluated and aligned with the safety and reliability requirements defined and applied within the TSP itself.
8) Outsourcing in a non-EU country is allowed only for those parts of the process that do not impact on the safety and reliability of the service (customer satisfaction, help desk, etc.).

2.6. Cloud infrastructures

With regard to the use of "cloud" infrastructures, the TSP shall:

1) give evidence of the capacity of real "operational control" of these services and of the guarantee of the location of the supporting technological infrastructure (physical servers to support the virtualized ones, "storage" and "backup" infrastructures, data transmission, BC and DR) allowed only within the EU;
2) ensure the transmission of data in a secure manner through any channel adopted;
3) provide evidence of the existence of the contractual right to carry out internal audit activities on these services that provides for the possibility of access also for the staff of QMSCERT, the Accreditation Body and the competent Supervisory Body. See point 4;
4) NOTE: The certification of the "cloud" service provider issued under accreditation, in the EA / MLA circuit, which covers the physical, logical and organizational perimeter referred to the TSP processes, against the ISO / IEC 27001 standard, corroborated by the use of the ISO 27017 Guideline, for the perimeter underlying the implementation of cloud services, including point-to-point communication lines, will be considered an acceptable way to consider the service compliant.
5) QMSCERT shall verify the existence of a risk assessment that integrates both the perimeter of the typical infrastructure of the TSP, and the perimeter consisting of the elements of cyberspace (communication in the broad sense) and those of the Cloud Service Provider;

6) ensure that physical data processing and storage infrastructures (including backups and other BC and DR resources) reside within the EU territory;
7) ensure that the management of personal data complies with the requirements of the GDPR (Regulation 679/2016) in both cases: proprietary infrastructure and "cloud" services.

2.7. Change management

TSP shall honor the following obligations:

1) Communicate any material changes to its infrastructure, processes or services to QMSCERT.
2) Autonomously prepare a risk analysis and subsequent planning process for the management of any significant change. TSP should ask QMSCERT and record the relevant communication in any case of doubt about deciding whether a change is considered significant or not.
3) Always communicate changes which have a direct impact on eIDAS services and/or information security infrastructure supporting this service.
4) Always declare the presence of remote signature HSMs/QSCDs in the TSP's infrastructure or at external structures operating within the responsibility of the TSP.

Any failure to comply with the above obligations, and any failures of information security which could compromise or could have compromised services, shall be classified and managed as a **major Non-Conformances**.

In detail:

TSP shall communicate any changes to its infrastructure or processes to QMSCERT. When this occurs, QMSCERT shall evaluate the impact of such changes, brought by the TSP, on its infrastructure or on the outsourcing of critical processes for services managed according to the requirements of the eIDAS Regulation. QMSCERT shall evaluate if such changes also regard the revisions of the TSP Practice Statements and/or of the SOA 27001 (where applicable).

If the TSP has not independently prepared a risk analysis and subsequent planning process for the management of change, QMSCERT shall record a **major Non-Conformance**.

The following are some indicative (not exhaustive) examples of what may be considered as a "significant change":

- changes to the configuration of the network infrastructure having an impact on the service or information security.
- changes to security policies and the technical modalities of their application.
- changes to the organizational structure of the management system.
- changes to the SOA or TSP Practice Statement.
- changes to the cryptographic devices (e.g., substitution of an HSM/QSCD providing a different type or level of security certification).
- elimination of organizational roles that affect security.
- others, as applicable.

On the other hand, factors not considered as significant changes include:

- normal staff turnover.
- normal maintenance operations that also involve component replacements.
- revision of a risk analysis if this does not involve changes in the application of operational control or process design.

In cases of doubt, TSP should better ask QMSCERT and record such communication.

Failure to communicate changes which have a direct impact on eIDAS services and/or information security infrastructure supporting this service, is to be considered a **major Non-Conformance** and shall be treated in a formal evaluation with records on the report, if such changes may cause a breach of security in the period between the application of these changes and the date of the audit being undertaken.

The TSP shall actively collaborate with these analyses. In serious cases, given the objective responsibility of QMSCERT with respect to the Accreditation Body and the Supervisory Body, QMSCERT informs the Accreditation Body in order to receive specific instructions. Information security deficiencies which may compromise or may have compromised services should always be classified as **major Non-Conformances**.

Failure to declare the presence of cryptographic devices (HSMs, remote QSCDs) in the TSP's infrastructure or at external structures operating within the responsibility of the TSP shall always be managed as a **major Non-Conformance**.

In the event of substantial changes to connected QERDS services, the TSP will also provide QMSCERT with the evidence of the new Test Report for interoperability, with a positive outcome, for the purposes of the continued validity of the Certificate of Conformity.

2.8. Termination

For the termination of qualified services, QMSCERT evaluates that the TSP applies the ENISA "Guidelines on Termination of Qualified Trust Services", published in December 2017, and any national-level requirements.

2.9. Special provisions

2.9.1. Registered delivery, preservation, and validation services

1. For **Electronic Registered Delivery Services (ERDS)**, ETSI EN 319 521 and, where applicable according to the characteristics of the trust service, ETSI EN 319 531 apply. Any waivers must be approved for each specific case by the Accreditation Body.
2. ETSI EN 319 522 and ETSI EN 319 532 are applicable according to the type of service.
3. If the service of the provider has **specific functional characteristics that do not comply with** ETSI EN 319 522/ETSI EN 319 532 in force, the following additional rules shall apply:

a. It is the responsibility of the TSP to provide all rational that demonstrate equivalence in terms of the requirements of the Regulation for the purpose of compliance assessment.
b. Specific indications issued or approved by a national Supervisory Body may be a valid element to take into account when assessing equivalence.
c. The rational with which equivalence is assessed must be documented and may be audited by the Accreditation Body for the purpose of confirming the accreditation of the body.
d. The number of days required will be assessed on a case-by-case basis, but it cannot be less than that provided by the applicable audit time rules.

4. For Qualified Electronic Seal and Signature **Preservation Services**, ETSI TS 119 511 applies. This specification is also generally applicable to preservation of data using digitally signed technologies.
   In the case of requests for certification other than the preservation of qualified electronic signatures and seals based on TS 119 511, the provisions of the next bullet point shall apply;
5. For Qualified Electronic Signature and Seal **Validation Services**, ETSI TS 119 441 and EN 319 102-1 and – if applicable by service type –TS 119 102-1 (which updates EN 319 102-1) and TS 119 102-2. The service must correctly use and validate trust lists based on TS 119 612 and TS 119 615, as well as correctly validate the certificates of the providers contained therein.
6. For **Registered Email Message (REM)** qualified delivery services offered by TSPs in Italy, see AgID - Technical rules for certified delivery services pursuant to eIDAS regulation no. 910/2014 - ETSI standard adoption criteria - REM Policy-IT Version 1.0 - 11.8.2022 and the additional guides and regulations of the aforementioned Authority that will be issued in the future.

2.9.2. National level identity proofing services

Identity proofing services pursuant to article 24, par.1(d) of the eIDAS Regulation are subject to national law/regulations and shall be audited accordingly by the CAB.[1]

For QTSPs offering such services, the evaluation shall be generally managed as part of the trust service. For example, certified QTSPs who wish to introduce such methods, shall apply to the CAB and shall be audited in accordance with the provisions specified in section 2.7 "*Change management*" of this regulation.

Non-TSPs offering such services (Identity Proofing Service Providers – IDSPs), may also apply for the certification of these services as a component of trust services. QTSPs may outsource identity proofing services to IDSPs only under the provisions specified in section 2.5 "*Outsourcing*" of this document. In this case, the audit of the QTSP who makes use of the identity proofing service

1 For Greece, the applicable regulation is the Decision of the Ministry of Digital Governance no.27499 EX 2021 which has been published in the Governmental Journal 3682/B/10-8-2021.

component shall include the trust services components interface (contractual, policy, procedural and technical wise). If the trust service uses a trust service component which has already been audited separately, the CAB 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 and the applicable certificate policy / practice statement. In case the IDSP has been audited by a different competent CAB, QMSCERT, as the receiving CAB, may make (partial or full) use of the results of that audit only after reviewing the entire dossier (certification documents, conformity assessment report).

Providers (TSPs, IDSPs) shall provide to the CAB all the necessary documentation of the identity proofing service prior to the evaluation of the implementation of the service by the CAB. They shall also provide evidence of the proper design, implementation and self-verification of the identity proofing service. The latter shall include detailed documentation of how the provider meets the requirements, in particular the national legislation/regulations, which apply in the scope of the identity proofing service (self-assessment checklist). Specialized standards (e.g. ETSI TS 119 461) and material (e.g. ENISA Remote ID Proofing report) should be followed/consulted in the design, implementation and self-verification of the service.

In case specialized software is utilized in integral parts of the identity proofing service (e.g. verification of document security characteristics, biometric checks, liveliness checks), the provider shall provide all the necessary documentation (certifications, audit results and/or test results) as evidence of the security, proper operation and effectiveness of that software. The audit team shall review the submitted documentation and, if necessary, it may request additional information/evidence, or checks (audit, tests, etc) at the expense of the provider (TSP, IDSP), which will provide sufficient guarantees that the applicable requirements are met. If cloud-based software services are utilized, the provisions of section 2.6 "*Cloud infrastructure*" of this document also apply.

3. Process requirements

3.1. Application process

3.1.1. Application

The organization shall apply for the certification of its Trust Services with the use of the applicable application form(s) from www.qmscert.com or using other means of information submission.

The organization shall determine ALL critical processes and performance indicators for the Trust Services it provides with regard to security and use, in its documented files, in agreement with the scope of certification and according to the applicable standards and/or regulations. The determination shall be based on regulatory, consumer, interested party and internal requirements of the organization.

3.1.2. Initial review

1. QMSCERT shall review the above information in order to verify possession of the specific competences to operate in the area of the services required.
2. The outcome of this analysis must give evidence of the feasibility of the activity to be planned (timing, skills of the Auditors and possible need for Experts)

3.1.3. Offer

Should the initial review result in verification of the feasibility of the audit activity (timing, skills of the Auditors and possible need for Experts) and determination of the audit time to conduct the audit, QMSCERT shall submit an offer that includes the commercial and certification terms.

For any new or updated applicable technical specification, the client will be notified of special requirements where appropriate before the initiation of the certification process and upon acceptance of the offer.

3.1.4. Acceptance and contract

Acceptance of the offer by the customer shall be done in writing (including email message) or other documented means.

A certification contract shall be communicated and signed by both parties (QMSCERT and the customer) following the offer acceptance. If there is already a valid certification contract between the two parties, acceptance of the offer by customer as described above may be considered sufficient.

3.1.5. Certification transfer

Transfers of certification shall be guaranteed only after a review of the entire dossier (previous reports going back at least two years) by QMSCERT as the receiving CAB, with an inspection of at least two working days at the TSP's head office and one day (one auditor) at each secondary/branch location where an HSM/QSCD is managed.

In cases of certification where any Non-Conformances have been raised within the last two-year period against the certification requirements, the inspection at the TSP shall have a duration not inferior to the duration of a non-regulated surveillance in order to verify the effectiveness of the corrective actions implemented. QMSCERT as the receiving CAB may take over the evaluation activities, in the ambit of validity of the existing certificate, only after it has approved its certification.

In case of a transfer from another CAB over renewal, the audit shall be conducted with 100% of the time of an initial verification.

3.1.6. Certification of components

With the publication of the ETSI EN 319 403-1 standard, the certification of specific trust service components, such as the Registration Authority service, is authorized.

3.2. Planning and execution

For the Planning and Execution of Audits, the Guidelines of Appendix A (in the corresponding applicable versions) are considered as reference documents.

3.2.1. Audit team

An audit team is appointed by QMSCERT to the audit activity, either during or following the initial review of the certification application. Based on availability of resources, the needs of the evaluation or other issues, the audit team may be adjusted.

3.2.2. Evaluation process

The Audit regarding related standards is conducted in two Stages.

3.2.2.1. Stage I Audit

The objective of Stage I is the collection of information necessary to be able to plan Stage II. Understanding the related standards and/or the technical file(s) of the Trust Services and all stages of production, the policy objectives where applicable and especially the level of readiness for audit.

Stage I can be conducted off-site or at the permanent locations of the organization. The activity ends with the issuance of a Stage I report signed by the customer.

The results of the Stage I audit include parts of the related standards and/or provision of the Trust Services that require attention and which can be declared as non-conformances in Stage II.

During Stage I, the maximum level of civil liability assumed by the TSP towards its customers will also be evaluated. At this level of liability, an appropriate insurance policy must be matched that considers the highest cumulative level of loss for a given event related to potential outages and the number of customers with the declared transaction value. QMSCERT will ask for evidence of the submission of insurance documents confirming the insurance coverage in progress to the Supervisory Body.

The Lead Auditor along with the customer will decide what is the required time to elapse for the audit of Stage II, considering the time required to resolve issues that have arisen during Stage I. Stage II planning can be modified depending on the findings of Stage I.

3.2.2.2. Stage II Audit

Stage II audit plan shall be prepared after and in-line with the findings / evidence gathered during Stage I. Stage II of the audit cannot be conducted immediately after the completion of Stage I, but with the appropriate time interval, agreed by the auditor and the customer, for implementing results of the Stage I audit.

Stage II audit will take place at the site(s) of the client organization with the purpose to evaluate the implementation and effectiveness of the client's Management System and Trust Service provision processes according to requirements of applicable standards and technical specifications, as these are published by interested parties (e.g. European Commission, CA-B Forum).

Any part of the related standards that has been fully audited during the Stage I audit may not need to be re-audited during Stage II. The Stage II audit report still will include findings that support conformance to requirements from audit findings during Stage I.

The audit team will collect evidence of any tests required to verify the results obtained by the Management System and/or service provisioning for similarity and reliability.

The audit team shall gather audit evidence that the Management System conforms to the standard and other certification requirements of related standards and technical specifications.

The audit team shall audit a sufficient number of examples of the activities of the client organization in relation to the Management System and activities to get a sound appraisal of the implementation and effectiveness of the Management System and Trust Service provisioning.

The audit team shall collect evidence that the provided services and products (certificates and timestamps) are in conformance with applicable requirements (i.e. certificate and timestamp profiles).

In the case of eIDAS audits, the audit team shall collect evidence that:

- the reporting of incidents to the relevant Supervisory Body is in accordance with article 19 of eIDAS Regulation.
- the requirements of the ENISA "Guidelines on Termination of Qualified Trust Services", published in December 2017, is adopted for the termination plan of qualified services.

In the case of audits which relate to the issuance of Publicly Trusted Certificates, such as TLS, Code-Signing, Email Protection, the audit team shall collect evidence of the handling of the TSP incidents that are documented in public repositories (e.g. Mozilla® Bugtracker) with an explanation of their remediation status, as applicable.The audit team shall address a sufficient number of the staff, including operational personnel and management of the audited facility to provide assurance that the system is implemented and understood within the organization.

Links between the normative requirements of related standards and technical specifications, performance objectives and targets, associated legal requirements, responsibilities and personnel competence, operations and procedures, performance data and internal audit results, as applicable, per critical process shall be audited.

The audit team shall analyze all information and audit evidence gathered during the Stage I and Stage II audits to determine the extent of fulfillment with all certification requirements and decide on the recommendation to be submitted for technical review and certification decision. The audit team may propose opportunities for improvement but shall not recommend specific solutions.

3.3. Findings

Findings can be categorized into the following levels:

1. Conforming
2. **Minor Non-Conforming** (requirement not met against the standard, or legislation or regulation or procedure of QMSCERT with **no impact** on performance and security of the product as well as the effectiveness of the Management System / Trust Services provisioning).
3. **Major Non-Conforming** (requirement not met against the standard, or legislation or regulation or procedure of QMSCERT with **impact** on performance and security of the product as well as the effectiveness of the Management System / Trust Services provisioning)

Opportunities for improvement (comments, recommendations, improvement ideas, etc.) of the management system or services are not allowed in the audit reports.

4. Audit results

4.1. Conformity Assessment Report

After audit completion, the Lead Auditor will compile a Conformity Assessment Report (CAR) according to the requirements set by ETSI EN 319 403-1, § 7.4.4.5 and the ETSI TS 119 403-3.

The CAR shall allow for evidence of the complete evaluation of all the applicable requirements and individual checks performed. The audit report shall include a compilation of the information gathered with the support of the applicable checklists (e.g. those attached to ETSI TR 119 411-4). QMSCERT's evaluation process shall cover the services which the TSP declared to the Supervisory Body.

Following QMSCERT's technical review and certification decision-making processes, the conformity to the eIDAS Regulation can be deliberated as well as the conformity of the services provided against the ETSI standards and/or other standards specifically identified by EA or by the European Commission for verifying the conformity of eIDAS services.

QMSCERT does not have to wait for the decisions of the Supervisory Body for the purposes of the decision with respect to certification or not of the TSP.

In the CAR, QMSCERT shall clearly indicate the conformity status to the accreditation scheme for the eIDAS Regulation 910/2014, in particular as stated in Articles 13, 15, 19, 24, 28, 29, 30 and from 32 to 45 and in the Annexes, where necessary, with the certified services, and also with the standard ETSI EN 319 401, where such conformity occurs.

The CAR gives evidence of the verification of all the operational controls in accordance with ETSI EN 319 401, specifying the frequency of monitoring activities by the TSP and the efficacy of such controls (ongoing records and the analysis of them, where possible).

The audit report highlights the effectiveness of the control of the TSP processes entrusted externally, especially for the identification and authentication processes (see also section 2.5 "*Outsourcing*").

The audit report also includes the Risk Assessment results (see section 2.2 "*Risk assesments*") and the Internal Audit results (see section 2.3 "*Internal audits*").

QMSCERT assures report's authenticity and integrity for interested parties with proper technical measures, including e-signing/e-sealing the CAR and/or uploading to QMSCERT's own web site.

Subsequently, the CAR, together with all the accompanying documents (e.g. checklists recording the objective evidence gathered on-site, ISO/IEC 27001 report), is formally submitted to the TSP which, in turn and if necessary, sends it in a timely manner to the Supervisory Body for the continuation of the process of qualification as QTSP.

In cases of annual surveillances not foreseen by the eIDAS Regulation but provided for under § 7.9 of the accreditation standards UNI CEI EN ISO/IEC 17065:2012 and ETSI EN 319 403-1, the report shall be managed in the same way as for the other regulated assessments, but the TSP is not required

to send the report to the Supervisory Body unless there is a specific request from the Supervisory Body itself.

4.2. Certificate of Conformity

The Certificate of Conformity issued by QMSCERT to the TSP shall contain references to the Accreditation Body's Regulation on eIDAS, as an accreditation scheme, and shall indicate compliance with the Regulation (EU) 910/2014 and the ETSI EN 319 401, the Standards relating to the Certified Services and the Services themselves. QMSCERT shall inform the TSP to send the Certificate of Conformity and the CAR to the Supervisory Body in a timely manner.

The Certificate of Conformity issued by QMSCERT to the TSP shall contain:

- References to the ACCREDIA Circular no.28/2023, as an Accreditation scheme;
- References to Regulation (EU) 910/2014 and ETSI EN 319 401;
- Conformity status to Articles 13, 15, 19, 24, 28, 29, 30 and from 32 to 45 and in the Annexes, as necessary according to the certified services.
- Compliance with the standards applicable to the Services subject to Certification and to the Services themselves, including the Regulations or similar documents of the competent Supervisory Bodies (e.g. EETT in Greece, AgID in Italy).

4.3. Notification of the Accreditation Body

QMSCERT takes care to upload the Certificate of Conformity on the Accredia webpage, and updates the certificate of conformity status in case of changes - revisions / withdrawal / suspension etc.

4.4. Notification of the Supervisory Body

QMSCERT takes care to remind the TSP to promptly send the Certificate of Conformity and the Conformity Assessment Report to the National Supervisory Body.

5. Certification Lifecycle

5.1. Regular audits

Full surveillance / re-certification audits shall be conducted every two years, and one partial surveillance in the years in which the complete audit is not carried out.

Partial surveillance shall always include the most critical processes and performance indicators for the provision of Trust Services. Given the impossibility, correlated with the timing of Surveillance Audits, to assess all applicable requirements with equal depth, QMSCERT plans against priority sampling criteria. The following is a non-exhaustive list of these criteria:

1. Closing of previous findings, if applicable.
2. New services and/or variation of services already provided, if applicable (Change management).
3. Evaluation of the performance of the services subject to certification (effectiveness and operational capacity).
4. New standards revisions, if applicable.
5. Context updates, risk analysis (in the face of accidents, changes in IT infrastructure and/or applications, etc.), outsourcing contracts, top management.
6. The outcome of Vulnerability Assessment/Penetration Test activities, and related Remediation Plans,
7. Security Incident Reporting and Management.
8. Any other issues applicable to the specific context and considered essential.

Refer to Appendix B – Surveillance audit requirements for guidance.

Depending on the above factors and the need to assess the closure and effectiveness of all audit results recorded in previous audits, QMSCERT may adjust surveillance audit times to the expense of the TSP.

Full surveillance audits may be conducted every year, if this is required for the customer to meet additional requirements, for example internal requirements or requirements of interested parties or for compliance with other standards, laws or regulations. Customer shall apply for this to QMSCERT with the use of an application form from www.qmscert.com or using other means of information submission.

For certificate issuance services which relate to international schemes that require annual comprehensive audits (i.e. Publicly Trusted Certificates, such as TLS, Code-Signing, Email Protection) the ETSI TS 119 403-2 applies as required.

Surveillance audits shall be conducted according to the requirements of Stage I and Stage II and related standard or regulation in a single Stage. The organization shall be notified with an audit schedule prior to the audit.

The audit team will examine the frequency and results of tests conducted under the Management System and/or the relevant standard or the relevant legislation in order to verify their effective implementation.

The Audit Groups called to operate for each TSP must be composed of 2 (two) competent eIDAS Auditors and any experts necessary to complete the coverage of the skills required by the Audit Group. In surveillance audits that go beyond the eIDAS Regulation (therefore, not biennial renewals), the audit team can be composed of only one Auditor.

5.2. Additional checks

QMSCERT is available to carry out any additional checks requested by the Supervisory Body, at the expense of the TSP and in accordance with the details of the request.

6. Appendix A – References

For the Planning, Planning and Execution of Audits, the following Guidelines in the corresponding applicable versions must be considered as reference documents:

1. Assessment of Standards related to eIDAS – December 2018: https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas
2. eIDAS: Overview on the implementation and uptake of Trust Services – January 2018: https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services
3. Recommendations for QTSPs based on Standards - Technical guidelines on trust services – December 2017: https://www.enisa.europa.eu/publications/reccomendations-for-qtsps-based-on standards/
4. Guidelines on Supervision of Qualified Trust Services - Technical guidelines on trust services – December 2017: https://op.europa.eu/en/publication-detail/-/publication/d94bbe97-3e5a-11ea-ba6e-01aa75ed71a1/language-en/format-PDF
5. Guidelines on Initiation of Qualified Trust Services - Technical guidelines on trust services – December 2017: https://www.enisa.europa.eu/publications/tsp-initiation
6. Conformity assessment of Trust Service Providers - Technical guidelines on trust services – December 2017: https://op.europa.eu/en/publication-detail/-/publication/c7669925-3e5a-11ea-ba6e-01aa75ed71a1/language-en/format-PDF/source-search
7. Security framework for Trust Service Providers - Technical guidelines on trust services – December 2017: https://www.enisa.europa.eu/publications/tsp-security
8. Security guidelines on the appropriate use of qualified electronic signatures - June 2017: https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures
9. Security guidelines on the appropriate use of qualified electronic seals – June 2017: https://op.europa.eu/en/publication-detail/-/publication/90d99ddb-d3de-11e6-ad7c-01aa75ed71a1/language-en/format-PDF/source-search
10. Security guidelines on the appropriate use of qualified electronic time stamps – June 2017: https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures
11. Security guidelines on the appropriate use of qualified website authentication certificates - June 2017: https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-website-authentication-certificates
12. Security guidelines on the appropriate use of qualified electronic registered delivery services – June 2017: https://op.europa.eu/en/publication-detail/-/publication/25a740dd-d3dd-11e6-ad7c-01aa75ed71a1/language-en/format-PDF
13. Regulations and Mandatory Circulars issued by the competent Supervisory Body (e.g. EETT for Greece, AgID for Italy), for specific services.

The Guidelines, in hypertext, referring to legal requirements, are applied in a mandatory manner.

7. Appendix B - Surveillance audit requirements

A surveillance audit requires an assessment of the closure and effectiveness of previous audit results as well as the assessment of applicable requirements against priority sampling criteria.

As a result, additional surveillance audit time may be required which QMSCERT will define based on the analyses of previous reports.

For the optimal planning of the audit and the determination of the sampling, QMSCERT requires the completion of the ANNEX F Part 2 from the customer before the initiation of the surveillance audit. The form addresses changes that occurred since the last audit and other information, such as:

- Overview of changes since the last audit
- Changes in the legal entity
- Changes in standards
- Changes in legislation
- New services
- Updates in existing services
- Changes in policies
- Changes in location
- Changes in cryptographic devices
- Organizational management changes
- Changes in personnel
- Changes in partners and contractors
- Changes in the infrastructure
- DR changes
- Changes in certificate profiles
- Changes in UTC(k) laboratories for timestamping
- Certificate statistics
- Risk management records (as attachment)
- Incidents