CERTIFICATION REQUIREMENTS OF TRUST SERVICE PROVIDERS (TSP)

Audit Information

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 relevant 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 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 319 522: Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings
- ETSI EN 319 532: Registered Electronic Mail (REM) Services; Part 4: Interoperability 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 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

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 Authority (EETT for Greece, AgID for Italy and so on) designated staff may also be present during these evaluations.

General Requirements:

1. Customer will apply for the certification of its Trust Services with the use of an application form from www.qmscert.com or using other means of information submission.
2. 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. QMSCERT shall review the above information in order to verify possession of the specific competences to operate in the area of the services required.
4. Where required by the regulations, standards and technical specifications, there will be documented procedures.
5. Completion and record of at least one full internal audit cycle for all applicable requirements of the related standards (when applicable).
6. Records that prove the application and implementation of the related standards shall exist (when applicable).
7. 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).

8. Objective evidence that the Trust Services provisioning processes are monitored and measured in relation to objectives for security and compliance.

Audit Expectations

Planning

The following Guidelines are considered as reference documents for the Planning and Execution of Audits, in the corresponding applicable versions:

- Assessment of Standards related to eIDAS – December 2018
- eIDAS: Overview on the implementation and uptake of Trust Services – January 2018
- Recommendations for QTSPs based on Standards - Technical guidelines on trust services – December 2017
- Guidelines on Supervision of Qualified Trust Services - Technical guidelines on trust services – December 2017
- Guidelines on Initiation of Qualified Trust Services - Technical guidelines on trust services – December 2017
- Conformity assessment of Trust Service Providers - Technical guidelines on trust services – December 2017
- Security framework for Trust Service Providers - Technical guidelines on trust services – December 2017
- Security guidelines on the appropriate use of qualified electronic signatures - June 2017
- Security guidelines on the appropriate use of qualified electronic seals – June 2017
- Security guidelines on the appropriate use of qualified electronic time stamps – June 2017
- Security guidelines on the appropriate use of qualified website authentication certificates - June 2017
- Security guidelines on the appropriate use of qualified electronic registered delivery services – June 2017
- Auditing Framework for TSPs – April 2015

The Audit regarding related standards is conducted in two Stages.

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 will be conducted as a preliminary audit and a documentation audit at the permanent locations of the organization.

The results of the audit of Stage I will be communicated to the client, including 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. Communication with the customer will include at a minimum:

- Evaluation of compliance of Trust Services with the requirements of the applicable technical standards and specifications
- Assessment of compliance according to applicable technical standards and specifications (where applicable)
- Evaluation of the conditions of the working environment of the customer and the security of the provisioned services
- Evaluation of critical processes and objectives when applicable
- Evaluation of the methodology of selected stages of the provision of the Trust Services and/or technical files and specifications of the provisioned Trust Services
- References to legislative requirements as well as associated risks to product security and requirements
- Assessment of the availability of resources
- Results or planning of internal audits and management review when applicable.

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 Authority.

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. **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

Stage II audit plan shall be prepared after and in-line with the findings / evidence gathered during Stage I.

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 Authority 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.

Presence of inspectors/observers of the Accreditation Body and/or Supervisory Authority
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.
In addition, the TSP accepts that both the Accreditation Body and the Supervisory Authority are able to intervene at all stages and at all sites and working environments, as observers, during compliance audits applicable to the scheme.

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)
4. Observation (a departure from a requirement/expectation, which raises a concern, but at the moment of the assessment it does not meet the criteria of a clear violation)

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

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 Authority.

Following QMSCERT's internal review, 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.
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. This wording shall also be present in the Certificate of Conformity.
QMSCERT staff shall assure report's authenticity and integrity for interested parties with proper technical measures; these may include e-signing/e-sealing the CAR and/or uploading to QMSCERT's own web site.
Subsequently, the CAR, together with all the documents recording the objective evidence gathered on-site, shall be formally submitted to the TSP which, in turn and if necessary, sends it in a timely manner to the Supervisory Authority for the continuation of the process of qualification as QTSP.
QMSCERT does not have to wait for the decisions of the Supervisory Authority for the purposes of the decision with respect to certification or not of the TSP. The CAR shall give 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).
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 Authority unless there is a specific request from the Supervisory Authority itself.

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 Authority in a timely manner.

Surveillance / Re-Certification 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:

a. Closing of previous findings, if applicable.
b. New services and/or variation of services already provided, if applicable (Change management).
c. New standards revisions, if applicable.
d. Context updates, risk analysis (in the face of accidents, changes in IT infrastructure and/or applications, etc.), outsourcing contracts, top management.
e. Vulnerability Assessment/Penetration Test Activities, and Related Remediation Plan
f. Security Incident Reporting and Management.

Miscellaneous applicable to the specific context and considered essential.
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.

Delivery, retention, and validation services

1. For delivery services, 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 from the Accreditation Body. ETSI EN 319 522 and ETSI EN 319 532 are applicable according to the type of service. 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 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 Authority 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.

2. For qualified electronic seal and signature preservation services, ETSI TS 119 511 applies.
3. 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 in them.

Cloud infrastructures

Regarding use of "cloud" infrastructures, the TSP shall provide evidence of its capacity for real "operational control" of these services and the guarantee of the location of the supporting technology infrastructure (servers, storage and data transmission infrastructures, such as VPNs) within the EU.
Retention data must always be transmitted in safe mode through the adopted channel(s).
The TSP must also give evidence of the existence of the contractual right to carry out internal audit activities on these services, which also provides for the access of CAB staff and the Supervisory Authority.
The existence of a "cloud" service provider certification issued under accreditation against ISO/IEC 27001, corroborated using the ISO 27017 guideline, for the underlying perimeter of cloud services, including point-to-point communication lines, will be considered an acceptable way to consider the service compliant.
Physical data processing and storage infrastructures must reside within the EU. The TSP shall apply the requirements of GDPR (Regulation 679/2016) in both cases: proprietary infrastructure and "cloud" services.

Evaluations of the robustness of IT Systems

QMSCERT shall verify the existence and acceptability of operational controls regarding VA (Vulnerability Assessment) and PT (Penetration Test) processes. The same can be carried out by structures inside or outside the TSP, or by structures inside or outside QMSCERT itself.
The internal organization of these Labs must be based on ISO/IEC 17025 and they must provide upfront evidence at least for the following:

- the clear identification and consistent application of the requirements involved in the methodology of technical evaluation used, preferably in accordance with ISO/IEC 27008;
- the formal competences (qualifications, issuer, sector experience) of personnel performing such tests;
- 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 of the TSP to be examined)

The above assessment, where the test laboratory is chosen by the TSP is the responsibility of the TSP and shall be validated as part of the audit process by QMSCERT. If, however, the laboratory has been chosen by QMSCERT the qualification rules applied are those set out in the accreditation standard ISO/IEC 17025.
The dates by which VA accredited LAB services must be adopted (and, subsequently, PT) will be subject to specific communications.

Outsourcing

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

Special Requirements per Technical Specification

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.

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

Obligations of the TSP - Changes to its infrastructure
In addition to the organization's obligations included in the main body of the certification contract, TSP shall honor the following obligations:

1. TSP shall communicate any changes to its infrastructure or processes to QMSCERT
2. TSP shall 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. TSP shall always communicate changes which have a direct impact on eIDAS services and/or information security infrastructure supporting this service
4. TSP shall 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.
If the TSP has not autonomously 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 infrastructure network having an impact on the service or information security;
- changes to security policies and the technical modalities of their application;
- modifications to the organizational set-up of the management system;
- a variation of the SOA or of the TSP Practice Statement;
- the substitution of an HSM/QSCD providing a different level of security certification;
- the 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 Authority, QMSCERT shall inform the Accreditation Body in order to receive specific instructions. Failures of information security which could compromise or could have compromised services shall always be classified as **major Non-Conformances**.
Failure to declare the presence of remote signature HSMs/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**.

Transfer of Certification
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.