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 requirements standards which fall under Reg. EU 2014_910 "eIDAS" and ETSI EN 319_403 accreditation scheme. These are:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

This regulation and all related documentation are subject to evaluations from designated staff of the Accreditation Body; state 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

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

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).
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.

Findings
Findings can be categorized into four 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. Opportunity/Proposal For Improvement

Audit Report
After audit completion, the Lead Auditor will compile an Audit Report according to the requirements set by ETSI

EN 319 403, § 7.4.4. Audit report shall allow for evidence of the complete evaluation of all the applicable requirements and single controls performed, incorporating in the same report the related ETSI checklists with the validation standards. QMSCERT's validation process shall cover the services which the TSP declared to the state 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 audit report, 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 Certificates of Conformity.
QMSCERT staff shall assure report's authenticity and integrity for interested parties with proper technical measures; these may include digitally signing the report or uploading to QMSCERT's own web site.
Subsequently, the report, together with all the documents recording the objective evidence gathered on-site, shall be formally sent to the TSP which, in turn and if necessary, sends it to the state authority 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, the report shall be managed in the same way as for the other regulated assessments, but TSP is not required to send the report to the state authority unless there is a specific request from the state authority itself.
QMSCERT does not have to wait for the decisions of the state authority for the purposes of the decision with respect to certification or not of the TSP. The audit report shall give evidence of the verification of all the operative 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, 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 state authority unless there is a specific request from the state 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, the accreditation scheme, and the Certificate shall show conformity to Reg. (EU) 910/2014 and to the standard ETSI EN 319 401, without further specifications regarding the services which are the subject of the qualification. The latter remains the final responsibility of the state authority.

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.
Full surveillance audits may be conducted every year, if this is required for the customer to meet additional requirements (i.e. internal requirements or by 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.
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.

Evaluations of the IT Systems
Regarding use of "cloud" infrastructures, the TSP shall provide evidence of his capacity for real operative control of these services.
QMSCERT shall verify the existence and acceptability of operative controls regarding VA (Vulnerability Assessment) and PT (Penetration Test) processes. These activities shall be done by internal or external laboratories with respect to the TSP, i.e. by internal or external persons to QMSCERT, whose qualification shall be based on, from June 1, 2017, the standard UNI CEI EN ISO/IEC 17025 and who shall provide evidence forthwith regarding at least:
- 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, source of issue of such, 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 with respect to their issue by the SOs and the applications of the Holder to be examined)

The above validation, 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 UNI CEI EN ISO/IEC 17065.
From June 1, 2018, operators performing PT and VA activities accreditation will become mandatory against the standard UNI CEI EN ISO/IEC 17025:2005.

Outsourcing
The following aply 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.
Using outsourcing modalities for the evaluation of TSPs performing such services, QMSCERT shall evaluate if "outsourcee" activities qualify as QTSPs (a qualification obtained in accordance with 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 assure the control of outsourced processes. The same is applicable for full outsourcing process controls.
In cases of QTSPs which allocate one or more HSMs at one or more clients, the QTSP shall ensure adequate operative monitoring and control criteria of such structures, ensuring the right to perform audits and authorized access for QMSCERT's auditors and for Accreditation Body and state authority observers.
Outsourcing of essential services (e.g. HSM management, database of CRL withdrawals management, management of the Registration Authority) is not allowed to be performed by operators who are not qualified (non-QTSP).

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

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 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**.

<u>In detail:</u>
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**. A significant change means a change to the infrastructure network having an impact on the service or information security, as well as changes to security policies and the technical modalities of their application. It could also mean 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 HMS providing for a different level of certification of security of the structure, or the elimination of organizational roles that affect security etc.
Factors not considered as significant changes include normal staff turnover, normal maintenance operations involving also the substitution of staff, or the revision of a risk analysis if this does not involve changes in the application of operative controls or in the planning of processes. 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 state 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 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) prepared by QMSCERT as the receiving CAB, with an inspection of at least two working days at the TSP's head office and one day at each secondary/branch location where an HSM device is in use.
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.

Please contact QMSCERT if you have any questions about this document