Technical Specifications on the Requirements for the operations of the Conformity Assessment Bodies, pursuant to the CSP Regulation

Version 1.0

25 February 2024

CHAPTER 1 – DEFINITIONS

1. ARTICLE 1 – Definitions and interpretation

The terms, words, and phrases used in these technical specifications shall have the same meaning as are ascribed to them in the Electronic Commerce and Transactions Law promulgated by Decree Law No. 16 of 2010 as amended or repealed and the Regulation of Certification Service Providers issued under CRA President Decision No. [X] of 2024 ("CSPs Regulation"), unless these specifications expressly provides for otherwise. For the purposes of these technical specifications, the following terms and words shall have the meanings ascribed to them below:

1.1 The terms listed below have the corresponding meanings:

State	State of Qatar.
The Authority	The Communications Regulatory Authority (CRA).
Committee	Grievance and Disputes Resolution Committee set out in Article (64) of the Law.
Law	the Electronic Commerce and Transactions Law promulgated by Decree Law No. 16 of 2010 or any amendment or law which repeals and replaces such law;
"CSPs Regulation"	Regulation on the Licensing and the Work of Certification Service Providers of 2024
Trust Service Provider (TSP)	A Certification Service Provider licensed to provide a trust service.
Trust Service (TS)	A service listed in paragraph 1 of Article (2) of the "CSPs Regulation", which is provided in accordance with the applicable requirements laid down in the "CSPs Regulation".
Qualified Trust Service Provider (QTSP)	A Certification Service Provider licensed to provide a qualified trust service, and which is granted a qualified status by the Authority.
Qualified Trust Service (QTS)	A service listed in paragraph 2 of Article (2) of the "CSPs Regulation", which is provided in accordance with the applicable requirements laid down in the "CSPs Regulation"
National Accreditation Body (NAB)	The sole body in the State or in a foreign country that performs accreditation with authority derived from the State or the foreign country.
Conformity assessment	An audit conducted to determine the extent of conformity of a target of evaluation with the conditions, controls and standards adopted pursuant to the "CSPs Regulation" and the decisions issued in implementation thereof.
Conformity Assessment Body (CAB)	The body that conducts a conformity assessment and produces a conformity assessment report based on the controls and conditions set by the Authority and fulfils the requirements of Article (18) of the" CSPs Regulation".
Conformity assessment report	The report resulting from a conformity assessment and issued by a conformity assessment body
Place of business	A non-transitory facility or installation used to carry out the business of an entity.

1.2 The Annexures to these Technical specifications form part of the technical specifications.

1.3 Unless otherwise expressly stated to the contrary in these technical specifications, any requirement for something to be communicated 'in writing' includes communication by email or any electronic process that the Authority introduces.

CHAPTER 2 – REQUIREMENTS FOR CONFORMITY ASSESSMENT BODIES

2. ARTICLE 2 – Requirements for conformity assessment bodies

2.1. With regards to the assessment of the conformity of trust service providers issuing certificates for website authentication (transport layer security certificates) and/or code signing certificates as a trust service with the requirements of the Law, of the "CSPs Regulation", and of the provisions and standards prescribed by applicable technical specifications of the Authority, in addition to the conformity assessment bodies referred to in paragraph 2.3, eligible conformity assessment bodies shall include WebTrust licensed international practitioners, that are duly licensed for conducting WebTrust for CA audits in the State.

2.2. Conformity assessment reports and certification attestations issued by conformity assessment bodies referred to in paragraph 2.1 shall conform to the WebTrust rules and shall confirm that the certification policies and certification practices statements of the trust service provider has been assessed to be in conformity with and abide by the requirements of the Law, the "CSPs Regulation", and of the provisions and standards prescribed by applicable technical specifications of the Authority.

2.3. With regards to the assessment of the conformity of trust service providers providing other types of trust services than the one referred to in paragraph 2.1 and of those trust service they provide with the requirements of the Law, of the "CSPs Regulation", and of the provisions and standards prescribed by applicable technical specifications of the Authority, eligible conformity assessment bodies shall be those bodies established in the State, accredited by the national accreditation body of the State as competent to conduct conformity assessment of the concerned type of trust service providers and trust service they provide, and approved by the Authority. Those conformity assessment bodies shall in particular engage technical auditors that:

2.3.1. Have thorough knowledge of the provisions of the Law, of the "CSPs Regulation", of these technical specifications, as well as of all the provisions and standards prescribed by applicable technical specifications of the Authority.

2.3.2. Hold a Certified Information Systems Auditor (CISA) certificate, Certified Information Technology Professional (CPA.CITP) certificate, Certified Internal Auditor (CIA) certificate or an accredited information security auditor certificate.

2.3.3. Have sufficient experience in the fields of electronic signatures, public key infrastructures, electronic programs, trust services, qualified trust service, information security tools and technology, security and financial reviews rules and specialized audit technologies.

2.3.4. Are able to conduct technical audit in compliance with the provisions and standards prescribed by applicable technical specifications of the Authority regarding the provision of trust services and of qualified trust services.

2.4. With regards to the assessment of the conformity of qualified trust service providers and of the qualified trust services they provide with the requirements of the Law, of the "CSPs Regulation", and of the provisions and standards prescribed by applicable technical specifications issued by the Authority, conformity assessment bodies shall be:

2.4.1. accredited by a national accreditation body being a signatory, either directly or through a regional body, of the International Accreditation Forum (IAF) or International Laboratory Accreditation Cooperation (ILAC) Multilateral Agreement;

2.4.2. under the [ISO/IEC 17065] framework supplemented by [ETSI EN 319 403-1];

2.4.3. for using an appropriate conformity certification scheme, which shall be established in accordance with [ISO/IEC 17067], in particular with its scheme type 6;

2.4.4. as competent to carry out conformity assessment and to provide conformity certification of qualified trust service providers and the qualified trust services they provide against the requirements of the Law, of the "CSPs Regulation" and of the provisions and standards prescribed by applicable technical specifications issued by the Authority; and

2.4.5. approved by the Authority.

2.5. Conformity assessment reports and certification attestations issued by conformity assessment bodies shall comply with the provisions laid down in Article 3.

CHAPTER 3 – CONFORMITY ASSESSMENT REPORTS

3. ARTICLE 3 – Requirements for conformity assessment reports

3.1. The conformity assessment report shall bear a clear certification decision, confirming - if such is the case - that the assessed QTSP and the QTS it provides or that the assessed TSP and the TS it provides meet all the applicable requirements of the Law, of the "CSPs Regulation", and of the provisions and standards prescribed by applicable technical specifications of the Authority.

3.2. The conformity assessment report shall provide sufficient details to demonstrate that the assessed QTSP/QTS or TSP/TS fulfil all the applicable requirements of the Law, of the "CSPs Regulation", and of the provisions and standards prescribed by applicable technical specifications of the Authority.

3.3. The conformity assessment report shall identify the name of the conformity assessment body, and where applicable its registration number, as stated in the official records, its official postal address, and its electronic address.

3.4. The conformity assessment report shall identify:

3.4.1. the name and country of the national accreditation body having accredited the conformity assessment body;

3.4.2. the link, on the official website of the national accreditation body, to the accreditation certificate issued by the national accreditation body to the conformity assessment body; and

3.4.3. when not mentioned in the accreditation certificate, the certification scheme for which the CAB has been accredited, as applicable:

a) under [ISO/IEC 17065] supplemented by [ETSI EN 319 403-1], to conduct conformity assessment of qualified trust service providers and the qualified trust services they provide; or

b) under which accreditation framework to conduct conformity assessment of trust service providers and the trust services they provide against the requirements of the Law, of the "CSPs Regulation", and of the provisions and standards prescribed by applicable technical specifications of the Authority.

3.5. The complete conformity assessment report and its annexes shall be considered as part of the certification documentation.

3.6. The conformity assessment report shall include the accredited conformity assessment (certification) scheme document (or set of documents) or a link to the location from where that document (or set of documents) is available.

3.7. The conformity assessment report shall bear qualified electronic signature(s) identifying the name and title of the conformity assessment body responsible person(s) having authorized the certification decision, or his/her handwritten signature.

3.8. The conformity assessment report shall be dedicated to one and only one trust service provider or qualified trust service provider, as applicable, in particular:

3.8.1. the conformity assessment report shall identify the name of the assessed provider, and where applicable its registration number (i.e., trade-license number and trade licensing authority in the State), as stated in the official records, its official postal address, and its electronic address; and

3.8.2. when applicable, the conformity assessment report shall identify this same information for all subsidiaries, affiliated legal entities and (sub)contractors that are operating service components in scope of the provision of trust service, or, as applicable, qualified trust service, by the provider, and hence in scope of the certification decision.

3.9. The conformity assessment report shall identify, in accordance with clause 5.5.3 of [ETSI TS 119 612], the service digital identity(ies) per type of trust service, or, as applicable, qualified trust service, for which the conformity assessment report confirms the conformity with the requirements of the Law, of the "CSPs Regulation" and of the provisions and standards prescribed by applicable technical specifications of the Authority, providing:

3.9.1. when the trust service, or, as applicable, the qualified trust service, is not PKI technology based, an identifier expressed as a URI that uniquely identifies the trust service, or, as applicable, the qualified trust service;

3.9.2. when the trust service, or, as applicable, the qualified trust service, is based on PKI technology, at least;

3.9.2.1. the Subject Key Identifier as defined in [IETF RFC 5280];

3.9.2.2. the Base64 PEM representation of the associated X.509-v3 digital certificate;

3.9.2.3. when applicable, an indication whether specific sets or subsets of end-entity certificates issued by or under the service digital identity are excluded or specifically included (e.g., as per transitional measures) from the certification decision and on the basis of which criteria they can be identified;

3.9.2.4. an indication whether the service digital identity relates to an end-entity or a certification authority, clarifying whether an issuing, intermediate or root; and

3.9.2.5. an indication on how the service digital identity is used in the context of the corresponding trust service, or, as applicable, the corresponding qualified trust service;

3.10. Per type of trust service, or, as applicable, qualified trust service, and for all service digital identities identified in paragraph 3.9, the conformity assessment report shall provide, if applicable, a detailed description of the public key infrastructure functional hierarchy with the purpose to allow identification of the service entry(ies) to be listed in the Qatar trusted list in accordance with the technical specifications of the Authority regarding the Qatar trusted list, including at least:

3.10.1. the illustration of the public key infrastructure hierarchy identifying the root certification authority(ies), the intermediate certification authority(ies), the issuing certification authority(ies) and the certification paths between them;

3.10.2. the identification of each certification authority illustrated in paragraph 3.10.1 through the Subject Key Identifier as defined in [IETF RFC 5280];

3.10.3. for each of the issuing certification authorities identified in paragraph 3.10.2, the list of the different (policy) sets of certificates such a certification authority is issuing, with for each set:

3.10.3.1. criteria that unambiguously identify the certificates of the set, being either a list of certificate policy identifiers to match with the content of the Certificate Policy certificate extension as defined in [IETF RFC 5280] or other criteria as defined in the technical specifications of the Authority regarding the Qatar trusted list;

3.10.3.2. an indication whether the certificates of the set are either qualified or not;

3.10.3.3. an indication whether the certificates of the set are either for electronic signatures, or for electronic seals, or for web site authentication or for none of these purposes and, in particular in this latter case, for which other purposes they are aimed to be used.

3.11. In line with paragraph 3.10, the conformity assessment report shall include:

3.11.1. an exhaustive list of third parties (e.g., subcontractors) which provide/operate service components of the trust service, or, as applicable, of the qualified trust service, by indicating their name, as identified in paragraph 3.8.2, together with the location of the sites where the corresponding component services are operated; and

3.11.2. an indication on which of these third parties and which sites have been subject to the audit and to which extent.

3.12. Pursuant the conclusions of the conformity assessment, the conformity assessment report shall provide an indication of the corresponding expected content of the Qatar trusted list, which reflects the result of the assessment.

3.13. The conformity assessment report shall identify the exhaustive list of public and internal documents of the trust service provider, or, as applicable, qualified trust service provider, including versioning of those documents, which have been part of the scope of the audit, including at least the following documentation for which a copy shall be either provided together with the report or made otherwise available to the Authority:

3.13.1. the declaration of the practices used by the provider, to provide the assessed trust service, or as applicable, qualified trust service;

3.13.2. the policy(ies) of the assessed trust service, or, as applicable, of the assessed qualified trust service, i.e., the set of rules that indicates the applicability of the trust service or qualified trust service to a particular community and/or class of application with common security requirements;

3.13.3. the terms and conditions related to subscriber agreements;

3.13.4. the termination plan;

3.13.5. the documentation related to the assessment of risks aimed at supporting the demonstration of fulfilment of the requirements of Article (21) of the "CSPs Regulation";

3.13.6. the security and personal data breach notification plan aimed at supporting the demonstration of fulfilment of the requirements of Article (22) of the "CSPs Regulation";

3.13.7. the list of all internal documents supporting the declaration of the practices referred to in paragraph 3.13.1 under the corresponding policy(ies) referred to in paragraph 3.13.2;

3.13.8. the memorandum and articles of incorporation and association of the assessed provider, in accordance with the applicable laws in the State, together with

3.13.8.1. Trade-license issued from the competent local authorities for the business activity (based on the type of the company) in the State;

3.13.8.2. Statement of business activities not relating to the provision of trust services, or, as applicable, qualified trust services;

3.13.8.3. Organizational chart;

3.13.8.4. Ownership structure information;

3.13.8.5. Report of the accounts auditor for the previous two years of the company, or from the date of its incorporation until the date of signing the conformity assessment report, whichever period is shorter.

3.13.9. the evidences that the assessed provider, in accordance with national laws, maintains sufficient financial resources and/or has obtained appropriate liability insurance with regards to the provision of the trust services, or, as applicable, of the qualified trust services;

3.13.10. the list of standards on the one side with which operations are claimed to be compliant and on the other side with which operations are certified to be compliant together with details about the underlying audit, evaluation, certification, or assessment scheme;

3.13.11. the list of qualified signature/seal creation devices and their certification related information when the assessed provider delivers such devices to its users; and

3.13.12. the list of devices used by the assessed provider as trustworthy devices (e.g., hardware security modules) to protect its own keys, and their certification related information, when the assessed provider uses such devices to secure the processes supporting the trust service, or, as applicable, the qualified trust service, it provides or aim to provide.

3.14. The conformity assessment report shall identify, for each stage of the audit (e.g., documentation audit and implementation audit including onsite inspections), the period during which the audit has been conducted (elapsed time) and the effort in man-days engaged by the conformity assessment body to conduct the audit.

3.15. Without prejudice of paragraph (4) of Article (17) of the "CSPs Regulation", the conformity assessment report shall provide, for each of the requirements of the Law, of the "CSPs Regulation" and of the

provisions and standards prescribed by applicable technical specifications of the Authority, an assessment report, with an indication of the non-conformities and their level of criticality, on the fulfilment by the assessed provider and the trust service, or, as applicable, the qualified trust service, it provides of the identified requirement, and/or when appropriate, on the existence of proper procedures and management system for handling this requirement

3.16. Referring to paragraph 3.15, the conformity assessment report shall identify, for each requirement, the detailed audit controls and control objectives that have been conducted during the audit with an indication of each non conformity and their level of criticality or include a reference to separately available audit reports in which such information is included, provided such separated reports are issued by other conformity assessment bodies that meet the requirements of the "CSPs Regulation" and of this Technical specifications and are endorsed by the conformity assessment body.

3.17. The conformity assessment report shall include the scope, the description, and the results of a significant set of test or production samples and their assessment for all relevant and applicable types of outputs from the assessed trust service, or, as applicable, from the assessed qualified trust service.

3.18. The conformity assessment report shall indicate:

3.18.1. by when, where applicable, the next surveillance audit must be conducted at the latest; and

3.18.2. by when the next compliance audit must be conducted at the latest.

3.19. The conformity assessment report shall contain an explicit declaration stating that the certification documents, including the conformity assessment report itself, are also intended for the use by the Authority.

CHAPTER 4 – APPROVAL OF CONFORMITY ASSESSMENT BODIES

4. ARTICLE 4 – Requirements for the approval of conformity assessment bodies

4.1. The Authority shall publish, on its website or by any other mean deemed suitable, all required information about the procedures and forms for the purposes of the approval of the conformity assessment bodies and for the purposes of the renewal of such an approval.

4.2. The conformity assessment body applying for an approval shall follow procedures and use application forms approved by the Authority.

4.3. The application for the approval of a conformity assessment body shall contain all information requested by the Authority. All information shall be submitted by the means determined by the Authority.

4.4. The Authority defines the documents and data that should be provided as part of the application referred to in paragraph 4.3, including at least:

4.4.1. A copy of the trade-license allowing the applicant to conduct business in the country in which it is established, or any equivalent extract of a trade register as in official records or registers of that country.

4.4.2. The business location, name, and where applicable the registration number of the applicant, as stated in the official records of the country in which it is established, together with identification data of those official records.

4.4.3. Financial reports for the last 3 years, that are issued by an authorized auditor in the country of establishment of the applicant, and that show financial capabilities of the applicant.

4.4.4. Evidences that the applicant fulfils the requirements referred to in Article 2.

4.5. The Authority may request additional documents and data, which are necessary to process the application.

4.6. Following its validation of the application, the Authority shall issue a Presidents Decision wherein it will either:

4.6.1. Approve the application if it concludes that the applicant complies with the requirements laid down in the Law, in the "CSPs Regulation", in these requirements and in all other relevant technical specifications issued by the Authority in implementation thereof, and with requirements of concerned authorities; or

4.6.2. Reject the application if it concludes that the applicant does not comply with the requirements laid down in the Law, in the "CSPs Regulation", in these requirements. , and in all other relevant technical specifications issued by the Authority in implementation thereof, and with requirements of concerned authorities.

4.7. If the Authority approves the application:

4.7.1. It shall grant an approval to the applicant for the scope indicated in the approval decision; and

4.7.2. It shall update the register of approved conformity assessment bodies in accordance with the approval decision, indicating the scope of approval as mentioned in the approval decision.

4.8. The approval is valid up to revocation by the Authority, conditioned to the fact that the approved conformity assessment body continues to meet the requirements of the Law, of the "CSPs Regulation", of these requirements, of concerned authorities, and of all other relevant technical specifications issued by the Authority in implementation thereof.

5. Article 5 – Suspension or revocation of the approval of conformity assessment bodies

5.1. The Authority may suspend the approval granted to a conformity assessment body when that body infringes one or more requirements of the Law of the "CSPs Regulation", of these technical specifications, of

concerned authorities, and of all other relevant technical specifications issued by the Authority in implementation thereof.

5.2. In case of suspension of the approval granted to a conformity assessment body, the Authority shall instruct the concerned conformity assessment body to stop immediately accepting trust service providers, or, as applicable, qualified trust service providers, established in the State as new customers for their conformity assessment services while continuing to serve their existing customers they contracted before the suspension decision. The concerned conformity assessment body shall act accordingly.

5.3. Where justified by the severity of the infringement(s) referred to in paragraph 5.1, or where those infringements are not remedied within three months of the suspension, the Authority shall revoke, without undue delay, the approval granted to a conformity assessment body.

5.4. In case of revocation of the approval granted to a conformity assessment body, or of its termination at the request by that body, the Authority shall instruct the concerned conformity assessment body to terminate immediately the contractual relationship it may have with trust service providers, or, as applicable, qualified trust service providers, established in the State, as customers for its conformity assessment services. The concerned conformity assessment body shall act accordingly.

5.5. In case of suspension or revocation of the approval granted to a conformity assessment body in accordance with these technical specifications, the Authority shall update the register of approved conformity assessment bodies accordingly.

6. ARTICLE 6 – Requirements for amending the approval of conformity assessment bodies

6.1. The conformity assessment body shall inform the Authority of changes to the information that was submitted during the application for approval, to the information appearing in the decision for granting an approval, including to its scope, within 14 calendar days from the occurrence of those changes.

6.2. Without prejudice to paragraph 6.1, the conformity assessment body shall communicate at least the following to the Authority:

6.2.1. Information about any change regarding the entity, ownership, and location of business of the conformity assessment body within its country of establishment.

6.2.2. Changes in the technical, financial, or management capability to operate and provide the services defined in the application or in the approval decision and the scope of the approval.

6.2.3. Any changes to the evidences of fulfilling the requirements referred to in Article 2 of this Technical specifications or with regards to the compliance with the requirements referred to in that Article 2.

6.2.4. A request for amending the scope of an existing approval granted to the conformity assessment body.

6.3. Any changes to an approval decision and its scope following the verification by the Authority of the relevant notified or requested changes shall be reflected in the register of approved conformity assessment bodies if the changes so require upon a decision from the Authority.

6.4. The Authority shall publish, on its website or by any other means deemed suitable, all required information about the procedures and forms for the purposes of the notification of changes related to the approval of conformity assessment bodies and the requests for their amendments.

CHAPTER 5 – REFERENCES

7. ARTICLE 7 – References

[ETSI EN 319 403-1]: ETSI EN 319 403-1 v2.3.1 (2020-06): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.

[ETSI TS 119 612]: ETSI TS 119 612 v2.1.1 (2015-07): Electronic Signatures and Infrastructures (ESI); Trusted Lists.

[IETF RFC 5280]: IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

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

[ISO/IEC 17067]: ISO/IEC 17067:2013, Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes**.**