Communications Regulatory Authority State of Qatar

هيئة تنظيم الاتصالات دولة قطر

Technical Specifications pursuant to Article 57 of the CSP Regulations for the trust service providers issuing certificates for website authentication and code signing

February 25, 2024

Article 1: Definitions

1. 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ascribed to them in the Electronic Commerce and Transactions Law promulgated by Decree Law No. 16 of 2010 as amended or repealed and the Regulation of Certification Service Providers issued under the Communications Regulatory Authority President Decision No. [X] of 2024 (”CSPs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:

“The Authority”	the Communications Regulatory Authority (“the CRA”);
“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 issued on the Licensing and activities performed by Certification Service Providers issued under CRA President Decision No. [X] of 2024 ;
“Conformity Assessment”	an audit conducted to determine the extent of conformity of a License applicant and Licensees with the conditions, controls and standards adopted under the Law, “CSPs Regulation” and the decisions issued in implementation thereof;
“Conformity Assessment Body” (CAB)	the body that conducts a Conformity Assessment based on the controls and conditions set by the Authority and fulfils the requirements of Article (18) of the “CSPs Regulation”;
“Conformity Assessment Report” (CAR)	the report resulting from a Conformity Assessment and issued by a Conformity Assessment Body;
“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”

"License"	an authorization issued pursuant to the provisions of the Law and its "CSPs Regulation", according to which a Licensee is allowed to carry out any of the Trust Services or Qualified Trust Services;
"Licensee"	a legal person who is licensed by the Authority in accordance with the provisions of the Law and its "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.
"The Qatar Trusted List"	the trusted list published by the Communications Regulatory Authority.

Article 2: Issuance of certificates for website authentication and code-signing

1. Pursuant to Article 57. of the "CSPs Regulation", trust service providers issuing certificates for website authentication and code signing shall comply with the requirements laid down in Annex I of these technical specifications.

Annex I: Technical requirements for trust service providers issuing certificates for website authentication and code signing

I.1 General requirements

1. The trust service provider issuing certificates for website authentication and code signing shall conform to [ETSI EN 319 401] amended according to [TSP-GEN] technical specifications.

2. The trust service provider issuing certificates for website authentication and code signing shall conform to the "Guidelines for The Issuance and Management of Extended Validation Certificate" [CABF Guidelines] and "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates" [CABF Baseline], appropriate to the type of certificate they provide, with the amendments provided in the subsequent articles of the present document, which have precedence on specifications from [CABF Guidelines] and [CABF Baseline];

I.2 Certificate policies and certification practice statement

1. The trust service provider's certification practice statement shall:
   i. shall be structured in accordance with [RFC 3647];
   ii. shall include the complete CA hierarchy, including root and subordinate CA's;
   iii. shall include the signature algorithms and parameters employed;
   iv. shall specify the practice regarding the use of CA keys for signing certificates, Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP);
   v. shall include a clear statement that where a trust service provider includes a hierarchy of subordinate CAs up to a root CA, the trust service provider shall be responsible for ensuring the subordinate-CAs comply with the applicable policy requirements

2. The trust service provider’s certificate policies and certification practice statement shall be identified by means of unique object identifiers of the form required in ITU-T Recommendation [X.509].

3. The corresponding trust service provider's own certificate profile identifier shall be included in the issued certificate.

4. The trust service provider shall publicly disclose its certification practice statement, its

certificate policy(ies) and their revisions through an online means that is available on a 24x7 basis.

5. The trust service provider shall publish PKI disclosure statement(s) that summarize key points of its certificate policy(ies) for the benefit of subscribers and relying parties.

6. The trust service provider shall publish an English translation of its certification practice statement, certificate policy(ies) and PKI disclosure statement(s).

7. The trust service provider's certificate policies shall specify the requirements for the use of certificate profiles.

I.3 Facility, Management, Operational and Security Controls

1. Requirements for the trustworthy systems shall be ensured by using systems conforming to [CEN TS 419 261] or to a suitable protection profile (or profiles), defined in accordance with [ISO 15408].

I.4 Issuance, management and revocation of certificates

1. Once a certificate is activated or accepted whichever event comes first, the trust service provider shall not proceed to the suspension of the certificate.

2. With regards to end-entity certificate rekey, the same rules apply as for the initial request.

3. With regards to end-entity certificate renewal, the trust service provider shall issue a new certificate using the subject’s previously certified public key, only if its cryptographic security is still sufficient for the new certificate’s validity period and no indications exist that the subject’s private key has been compromised nor that the certificate has been revoked due to any other security breach.

4. With regards to end-entity certificate modification, the same rules apply as for the initial request.

I.5 Provisions related to the inclusion of the issuance of certificates for website authentication and code signing trust service in the Qatar trusted list

1. A trust service consisting in the issuance of certificates for website authentication and code

signing is identified in the Qatar trusted list by means of the digital certificate of a root-CA, an intermediate CA or an issuing CA.

2. The confirmation by a conformity assessment body approved by the Authority and the verification by the Authority of the conformity of the trust service provider and the trust service it provides with the requirements of the Law, of the “CSPs Regulation” and of the applicable technical controls of the Law and the “CSPs Regulation” shall allow the demonstration that under the CA identified in the first paragraph above, it is possible to distinguish without any ambiguity qualified certificates from certificates for website authentication and code signing, and certificates for electronic signatures from certificates for electronic seals and from certificates for website authentication and code signing.

3. The trust service provider shall not include in certificates for website authentication or code signing any data or attribute that might lead to identifying them erroneously as qualified.

References

Reference	Title
[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]	The Regulation on the Licensing and the Work of Certification Service Providers of 2024
[TSP-GEN]	Technical Specifications on the General Requirements issued pursuant to Certified Service Providers Regulations on technical controls applicable to trust service providers or qualified trust service providers and the trust services or qualified trust services provided.
[X.509]	ISO/IEC 9594-8/Recommendation ITU-T X.509: Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks.
[RFC 3647]	IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework
[ETSI EN 319 401]	ETSI EN 319 401 v2.3.1 (2021-05): Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[CEN TS 419 261]	CEN TS 419 261: Security requirements for trustworthy systems managing certificates and time stamps
[CABF Guidelines]	CA/Browser Forum: Guidelines for The Issuance and Management of Extended Validation Certificates
[CABF Baseline]	CA/Browser Forum: Baseline Requirements Certificate Policy for the Issuance and Management of Publicly Trusted Certificates
[ISO 15408]	ISO/IEC 15408 (parts 1 to 3): Information technology - Security techniques - Evaluation criteria for IT security