Communications Regulatory Authority State of Qatar

هيئة تنظيم الاتصالات دولة قطر

Technical Specifications pursuant to Articles 41.9 & 48.10 for the *Specific provisions for (Qualified) trust service providers issuing (Qualified) certificates for electronic signatures or for electronic seals*

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ascribed to them in the Electronic Commerce and Transactions Law promulgated by Decree Law No. 16 of 2010 as amended or repealed and the Regulation of Certification Service Providers issued under the Communications Regulatory Authority President Decision No. [X] of 2024 (”CSPs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 on the Licensing and the 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.
"Qatar Trusted List"	The trusted list published by the Communications Regulatory Authority

Article 2: Issuance of certificates for electronic signatures or for electronic seals

1. Pursuant to Article (41.9) and Article (48.10) of the "CSPs Regulation", trust service providers issuing certificates for electronic signatures or for electronic seals shall comply with the requirements laid down in Annex I of these technical specifications.

Article 3: Issuance of qualified certificates for electronic signatures or for electronic seals

1. Pursuant to Article 41.9 and article 48.10 of the "CSPs Regulation", qualified trust service providers issuing qualified certificates for electronic signatures or for electronic seals shall comply with the requirements laid down in Annex IV of these technical specifications.

Annex I: Technical requirements for trust service providers issuing certificates for electronic signatures and/or for electronic seals

I.1 General requirements

1. The trust service provider issuing certificates for electronic signatures or certificates for electronic seals shall conform to [ETSI EN 319 411-1] with the amendments provided in the subsequent clauses of the present Annex, which have precedence over specifications from [ETSI EN 319 411-1].

2. All mentions of “trust service provider” in [ETSI EN 319 411-1] shall be understood as “trust service provider or qualified trust service provider as defined in the [“CSPs Regulation”]”, including all mentions present in the amendments provided in the present annex.

3. All mentions of “trust service” in [ETSI EN 319 411-1] shall be understood as “trust service or qualified trust service as defined in the [“CSPs Regulation”]”, including all mentions present in the amendments provided in the present annex.

4. All references to [ETSI EN 319 401] made directly or indirectly in [ETSI EN 319 411-1] shall be understood as referring to the version of that standard amended according to [TSP-GEN] Technical specifications.

5. All references to [ETSI EN 319 412-2] made directly or indirectly in [ETSI EN 319 411-1] shall be understood as referring to the version of that standard amended according to Annex II of these technical specifications.

6. All references to [ETSI EN 319 412-3] made directly or indirectly in [ETSI EN 319 411-1] shall be understood as referring to the version of that standard amended according to Annex III of these technical specifications.

I.2 Certificate policies and certification practice statement

1. OVR-5.2-02 of [ETSI EN 319 411-1] is amended so it reads: “The trust service provider's certification practice statement shall be structured in accordance with IETF RFC 3647”.

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 Recommendation [X.509].

3. OVR-5.2-05 of [ETSI EN 319 411-1] is amended so it reads: "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."

4. 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.

5. The PKI disclosure statement(s) shall be structured in accordance with Annex A of [ETSI EN 319 411-1]

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. The recommendation in OVR-6.4.4-02 of [ETSI EN 319 411-1] is turned into an obligation (i.e. the term "should" is replaced by "shall").

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 electronic signatures or for electronic seals trust services in the Qatar trusted list

1. A trust service consisting in the issuance of certificates for electronic signatures or for electronic seals 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” must 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, and certificates for electronic signatures from certificates for electronic seals and from certificates for website authentication and code signing, and qualified certificates for electronic signatures from qualified certificates for electronic seals.

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

Annex II: Content profile for certificates for electronic signatures

II.1 Generic requirements

1. Certificates for electronic signatures shall conform to [ETSI EN 319 412-2] to the exception of section 5 and with the amendments provided in all the subsequent clauses of the present Annex.

II.2 Basic certificate fields

II.2.1 Issuer

II.2.1.1 Legal person issuers

1. GEN-4.2.3.1-2 of clause 4.2.3.1 of [ETSI EN 319 412-2] is amended to add the following item to the list: "`organizationIdentifier` in compliance with [ETSI EN 319 412-1] clause 5.1.4".

II.2.2 Subject

1. NAT-4.2.4-6 of clause 4.2.4 of [ETSI EN 319 412-2] is amended so it reads: "When a natural person subject is associated with an organization, the subject attributes shall also identify such organization using the attributes:
   i. `organizationName` including the full name of the organization as stated in the official records, and
   ii. `organizationIdentifier` including the registration number as stated in the official records."

2. The value of the `organizationIdentifier` attribute shall be structured as follows: NTRQA-TradeLicense# where "TradeLicense#" is a trade license identifier allocated to the organization by the applicable Trade Licensing Authority.

II.2.3 NotAfter

NOTE: This clause is not specified in [ETSI EN 319 412-2].

1. The end of the validity period (the date indicated in the field "`NotAfter`") of an end-entity certificate shall not exceed the end of the validity period (the date indicated in the field

"NotAfter") of the certificate of the issuing CA.

II.2.4 Standard certificate extensions

II.2.4.1 Key usage

1. The Key Usage Type A, as specified in clause 4.3.2 of [ETSI EN 319 412-2], shall be used exclusively.

II.2.4.2 Certificate policies

1. GEN-4.3.3-2 of clause 4.3.3 of [ETSI EN 319 412-2] is amended so that it reads: "The certificate policies extension shall be present and shall contain the identifier of at least one certificate policy which reflects the practices and procedures undertaken by the CA and that is established and managed by the CA."

II.2.5 Qatar QcStatements

1. Certificates that have been issued as certificates for electronic signature shall contain the QcType 1 QcStatement described in clause 4.2.3 of [ETSI EN 319 412-5].

2. Declaration of a limitation on the value of transaction for which a certificate can be used, shall be implemented by means of the declarative QcStatement statement specified in clause 4.3.2 of [ETSI EN 319 412-5].

3. Declaration of a retention period for material information relevant to the use of and reliance on a certificate, shall be implemented by means of the declarative QcStatement statement specified in clause 4.3.3 of [ETSI EN 319 412-5].

4. URLs to the applicable PKI Disclosure Statements (PDS) in accordance with Annex A of [ETSI EN 319 411-1] shall be implemented in conformance with clause 4.3.4 of [ETSI EN 319 412-5].

Annex III: Content profile for certificates for electronic seals

III.1 Generic requirements

1. Certificates for electronic seals shall conform to [ETSI EN 319 412-3] with the amendments provided in the subsequent clauses of the present Annex.

2. All references to [ETSI EN 319 412-2] made directly or indirectly in [ETSI EN 319 412-3] shall be understood as referring to the version of that standard amended according to Annex II, including the exclusion of section 5, of these technical specifications.

III.2 Basic certificate fields

III.2.1 Subject

1. LEG-4.2.1-5 of clause 4.2.1 of [ETSI EN 319 412-3] is amended so it reads:
"The `organizationName` shall include the full name of the organization as stated in the official records."

2. LEG-4.2.1-6 of clause 4.2.1 of [ETSI EN 319 412-3] is amended so it reads:
"The `organizationIdentifier` shall include, in compliance with clause 5.1.4 of [ETSI EN 319 412-1], the organization's registration number as stated in the official records."

III.3 Standard certificate extensions

III.3.1 Key usage

1. The Key Usage Type C or D as specified in clause 4.3.2 of [ETSI EN 319 412-2] shall be used to the exclusion of any other combination.

III.3.2 Certificate policies

1. GEN-4.3.3-2 of clause 4.3.3 of [ETSI EN 319 412-2] is amended so that it reads: "The certificate policies extension shall be present and shall contain the identifier of at least one certificate policy which reflects the practices and procedures undertaken by the CA and that is established and managed by the CA."

III.4 Qatar QcStatements

1. Certificates that have been issued as certificates for electronic seals shall contain the QcType 2 QcStatement described in clause 4.2.3 of [ETSI EN 319 412-5].

Annex IV: Technical requirements for qualified trust service providers issuing qualified certificates for electronic signatures or for electronic seals

IV.1 Introduction

The present Annex defines four (4) certificate policies:

1) A policy for Qatar (QA) qualified certificates issued to natural persons (QA-QCP-n) offering the level of quality defined in the “CSPs Regulation” for QA qualified certificates. The identifier for this policy is: OID_QA_QCP_N
2) A policy for QA qualified certificates issued to legal persons (QA-QCP-l) offering the level of quality defined in the “CSPs Regulation” for QA qualified certificates. The identifier for this policy is: OID_QA_QCP_L
3) A policy (QA-QCP-n-qscd) for QA qualified certificates issued to natural persons offering the level of quality defined in the “CSPs Regulation” for QA qualified certificates and requiring the use of a QA Qualified Signature Creation Device (QSCD). The identifier for this policy is: OID_QA_QCP_N_QSCD
4) A policy (QA-QCP-l-qscd) for QA qualified certificates issued to legal persons offering the level of quality defined in the “CSPs Regulation” for QA qualified certificates and requiring the use of a QA Qualified Seal Creation Device (QSCD). The identifier for this policy is: OID_QA_QCP_L_QSCD

The requirements applicable to the services offered under one of those certificate policies are indicated by clauses marked by the applicable certificate policy indicator: "[QA-QCP-l]", "[QA-QCP-n]", "[QA-QCP-l-qscd]" and/or "[QA-QCP-n-qscd]"

The requirements applicable to any CP (Certificate Policy) are indicated by clauses without any additional marking.

IV.2 General requirements

1. Qualified certificates for electronic signatures not intended to support the creation of qualified electronic signatures shall be issued under the [QA-QCP-n] requirements.

2. Qualified certificates for electronic seals not intended to support the creation of qualified electronic seals shall be issued under the [QA-QCP-l] requirements.

3. Qualified certificates for electronic signatures intended to support the creation of qualified electronic signatures shall be issued under the [QA-QCP-n-qscd] requirements.

4. Qualified certificates for electronic seals intended to support the creation of qualified electronic seals shall be issued under the [QA-QCP-l-qscd] requirements.

5. [QA-QCP-n]: All requirements defined in [ETSI EN 319 411-2] for the certificate policy [QCP-n] shall apply with the amendments provided in the subsequent clauses of the present Annex, which shall prevail over the corresponding requirements of the former.

6. [QA-QCP-l]: All requirements defined in [ETSI EN 319 411-2] for the certificate policy [QCP-l] shall apply with the amendments provided in the subsequent clauses of the present Annex, which shall prevail over the corresponding requirements of the former.

7. [QA-QCP-n-qscd]: All requirements defined in [ETSI EN 319 411-2] for the certificate policy [QCP-n-qscd] shall apply with the amendments provided in the subsequent clauses of the present Annex, which shall prevail over the corresponding requirements of the former.

8. [QA-QCP-l-qscd]: All requirements defined in [ETSI EN 319 411-2] for the certificate policy [QCP-l-qscd] shall apply with the amendments provided in the subsequent clauses of the present Annex, which shall prevail over the corresponding requirements of the former.

9. All mention of "Regulation (EU) No 910/2014" in [ETSI EN 319 411-2] shall read "[”CSPs Regulation”]".

10. All mention of "EU qualified certificates" in [ETSI EN 319 411-2] shall read "Qatar qualified certificates".

11. All mention of “(EU) qualified electronic signatures” and “(EU) qualified electronic seal” in [ETSI EN 319 411-2] shall read respectively as “Qatar qualified electronic signatures” and to “Qatar qualified electronic seal”.

12. All references to [ETSI EN 319 401] made directly or indirectly in [ETSI EN 319 411-2] shall be understood as referring to the version of that standard amended according to [TSP-GEN] technical specifications.

13. All references to [ETSI EN 319 411-1] made in [ETSI EN 319 411-2] shall be understood as referring to the version of that standard amended according to Annex I of these technical specifications and as applicable mutatis mutandis to qualified trust service providers issuing qualified certificates for electronic signatures or for electronic seals.

14. All references to [ETSI EN 319 412-2] made in [ETSI EN 319 411-2] and [ETSI EN 319 411-1] shall be understood as referring to the version of that standard amended according to Annex V of the present document.

15. All references to [ETSI EN 319 412-3] made in [ETSI EN 319 411-2] and [ETSI EN 319 411-1] shall be understood as referring to the version of that standard amended according to Annex VI of the present document.

IV.3 Issuance, management and revocation of qualified certificates

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

2. Requirement **IDV-1**: Identity verification, ensuring the "identification of the person with a high level of confidence", procedure shall be followed where a method providing "at a minimum a reliable guarantee and equivalent assurance in terms of reliability to personal attendance" shall be limited to:
    a. The use of electronic identification tools that are listed in the Authority's register of approved electronic identification tools provided they are listed as meeting the requirements for providing a high level of assurance with regards to the identity of the person to whom the qualified certificate is issued;
    b. The use of qualified certificates supporting a qualified electronic signature or a qualified electronic seal for the verification of the identity prior the delivery of a qualified certificate for electronic signature or of a qualified certificate for electronic seal respectively. In that case:
        i. The qualified electronic signature or qualified electronic seal must have been created on the electronic document used to request the new qualified certificate and including all the required information for the delivery of the qualified certificate,
        ii. The qualified trust service provider must implement a process for the

validation of the qualified electronic signature or qualified electronic seal in accordance with the "CSPs Regulation" or make use of a qualified validation service for the validation of qualified electronic signature or qualified electronic seal in accordance with the "CSPs Regulation".

c. Any other identification procedure provided:

i. It is confirmed by an Authority-approved conformity assessment body that the implementation of that procedure by the qualified trust service provider provides a high level of assurance with regards to the identity of the person to whom the qualified certificate is issued;

ii. This confirmation demonstrates the implementation of technical and organizational measures mitigating the risks of fraud and impersonation with an efficiency corresponding to a high level of assurance, and mitigating the risks related to the tampering, fraudulent manipulation or handling of communication channels (including audio and video communications);

iii. The procedure is verified and approved by the Authority or its delegate prior its implementation in production.

3. REG-6.2.3-01 of [ETSI EN 319 411-2] is amended so it reads:

"The requirements identified in ETSI EN 319 411-1 [2], clause 6.2.3 and the requirement **IDV-1** shall apply."

4. REG-6.3.8-02 of [ETSI EN 319 411-1] is amended so it reads:

"If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information shall be verified, recorded, agreed to by the subscriber in accordance with clauses REG-6.3.1-00B, 6.2.2 and **IDV-1**."

5. OVR-6.3.4-02 of [ETSI EN 319 411-2] is amended so it reads:

"If the subscriber agreement is in electronic form, it should be signed with a Qualified Electronic Signature or a Qualified Electronic Seal as specified by ["CSPs Regulation"] "

IV.4 Provisions related to the inclusion of the issuance of qualified certificates for electronic signatures or for electronic seals qualified trust services in the Qatar trusted list

1. A qualified trust service consisting in the issuance of qualified certificates for electronic

signatures or for electronic seals 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 qualified trust service provider and the qualified 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, and certificates for electronic signatures from certificates for electronic seals and from certificates for website authentication and code signing, and qualified certificates for electronic signatures from qualified certificates for electronic seals.

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

Annex V: Content profile for qualified certificates for electronic signatures

V.1 Generic requirements

1. All certificate fields and extensions shall comply with [ETSI EN 319 412-2] with the amendments specified in Annex II of these technical specifications with the additional amendments of the present Annex.

V.2 QA Qualified Certificate requirements

V.2.1 QA QCStatements

1. When certificates are issued as Qatar qualified certificates, they shall include QCStatements in accordance with [ETSI EN 319 412-5] amended as specified in subsequent clauses of this section.

2. When certificates are issued as Qatar qualified certificates, they shall include URLs to the applicable PKI Disclosure Statements (PDS) in conformance with clause 4.3.4 of [ETSI EN 319 412-5].

V.2.2 Certificate policies

1. The policy identifiers defined in clause 5.3 of [ETSI EN 319 411-2] shall not be included in end-entity certificates.

2. When certificates are issued as Qatar qualified certificates, they shall include one of the OIDs corresponding to the certificate policies defined in Annex IV of the present document.

Annex VI: Content profile for qualified certificates for electronic seals

VI.1 Generic requirements

1. All certificate fields and extensions shall comply with [ETSI EN 319 412-3] with the amendments specified in Annex III of these technical specifications with the additional amendments of the present Annex.

2. All references to [ETSI EN 319 412-2] made in [ETSI EN 319 412-3] shall be understood as referring to the version amended according to Annex V of these technical specifications.

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
[ETSI EN 319 411-1]	ETSI EN 319 411-1 v1.4.1 (2023-10): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI EN 319 411-2]	ETSI EN 319 411-2 v2.5.1 (2023-10): 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]	ETSI EN 319 412-1 v1.5.1 (2023-09): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[ETSI EN 319 412-2]	ETSI EN 319 412-2 v2.3.1 (2023-09): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[ETSI EN 319 412-3]	ETSI EN 319 412-3 v1.3.1 (2023-09): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[ETSI EN 319 412-5]	ETSI EN 319 412-5 v2.4.1 (2023-09): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements