Technical Specifications pursuant to Articles 40.4, 40.6, 46.4 and 46.6 of the CSP Regulations for the Specific provisions for (Qualified) trust service providers providing the remote creation of (Qualified) electronic signatures or 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ascribed to them in the Electronic Commerce and Transactions Law promulgated by Decree Law No. 16 of 2010 as amended or repealed and the Regulation of Certification Service Providers issued under the Communications Regulatory Authority President Decision No. [X] of 2024, unless these specifications expressly provide 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 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: Remote creation as a service of electronic signatures and advanced electronic signatures as a trust service

1. Pursuant to Article (40.4) of the "CSPs Regulation", trust service providers providing the remote creation as a service of electronic signatures and advanced electronic signatures as a trust service shall comply with the requirements laid down in Annex I of these technical specifications.

Article 3: Remote creation as a service of electronic seals and advanced electronic seals as a trust service

1. Pursuant to Article (46.4) of the "CSPs Regulation", trust service providers providing the remote creation as a service of electronic seals and advanced electronic seals as a trust service shall comply mutatis mutandis with the requirements laid down in Annex I of these technical specifications.

Article 4: Remote creation as a service of qualified electronic signatures as a qualified trust service

1. Pursuant to Article (40.6) of the "CSPs Regulation", qualified trust service providers providing the remote creation as a service of qualified electronic signatures as a qualified trust service shall comply with the requirements laid down in Annex II of these technical specifications.

Article 5: Remote creation as a service of qualified electronic seals as a qualified trust service

1. Pursuant to Article (46.6) of the "CSPs Regulation", qualified trust service providers providing the remote creation as a service of qualified electronic seals as a qualified trust service shall comply mutatis mutandis with the requirements laid down in Annex II of these technical specifications.

Annex I: Technical requirements for trust service providers providing the remote creation as a service of electronic signatures and advanced electronic signatures.

I.1 General requirements

1. The trust service provider providing the remote creation as a service of electronic signatures and advanced electronic signatures as a trust service shall conform to [ETSI TS 119 431-2] with the amendments provided in the subsequent clauses of the present Annex, which have precedence on specifications from [ETSI TS 119 431-2].

2. All references to ETSI EN 319 401 made directly or indirectly in [ETSI TS 119 431-2] shall be understood as referring to the version of that standard amended according to [TSP-GEN] Technical Specifications.

3. All references to ETSI EN 319 411-1 made directly or indirectly in [ETSI TS 119 431-2] shall be understood as referring to the version of that standard amended according to Annex I of [TSP-CA] Technical Specifications.

4. All mentions of "trust service provider" in [ETSI TS 119 431-2] 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.

5. All mentions of "trust service" in [ETSI TS 119 431-2] 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.

6. All mentions of "Regulation (EU) No 910/2014" in [ETSI TS 119 431-2] shall read "["CSPs Regulation"]".

7. All mentions of "(EU) qualified electronic signatures" and "(EU) qualified electronic seal" in [ETSI TS 119 431-2] shall read respectively as "Qatar qualified electronic signatures" and to "Qatar qualified electronic seals" as defined in the ["CSPs Regulation"].

8. All mentions of "EUMS trusted list" in [ETSI TS 119 431-2] shall read as "Qatar trusted list" as defined in the ["CSPs Regulation"].

I.2 Trust service practice statement

1. The trust service provider's remote signature creation service policies and practice statement(s) shall be established and structured in accordance with [ETSI TS 119 431-2], in particular its Annex A.

2. The trust service provider's remote signature creation service practice statement shall specify all the supported protocols for remote electronic signature creation.

3. The trust service provider's remote signature creation service practice statement shall specify if the to-be-signed document can be provided only as a hash.

4. The trust service provider's remote signature creation service policies and practice statement(s) shall be identified by means of unique object identifiers of the form required in ITU-T Recommendation [X.509].

5. The trust service provider shall publicly disclose its remote signature creation service policies and practice statement(s) and their revisions through an online means that is available on a 24x7 basis.

6. The trust service provider shall publish a remote signature creation service disclosure statement(s) that summarize key points of its service policy(ies) for the benefit of subscribers and relying parties.

7. The trust service provider shall publish an English translation of its remote signature creation service policies, practice statements, and disclosure statements.

I.3 Signature creation application service component technical requirements

1. Protocols for remote electronic signature creation used to communicate with the solution should comply with [ETSI TS 119 432] or [CSC API] specifications.

2. The solution should offer remote signing capabilities directly to the end-user, via a user portal where he can upload and sign a document and download the signed result.

   Note: This requirement ensures that an end-user can sign in a standalone way, i.e., independently of a pre-existing integration with a service provider.

3. The solution shall at least support the creation of:

    - XAdES digital signatures in compliance with [ETSI EN 319 132-1].

    - PAdES digital signatures in compliance with [ETSI EN 319 142-1].

4. The creation of AdES digital signatures shall comply with [ETSI EN 319 102-1].

5. The supported levels shall at least include -B and -T.

I.4 Provisions related to the inclusion of the remote creation as a service of electronic signatures and advanced electronic signatures as a trust service in the Qatar trusted list

1. The trust service provider shall have for each instance of the trust service it provides, one service digital identifier as defined in clause 5.5.3 of [ETSI TS 119 612] which allows to identify the service uniquely and unambiguously within the Qatar trusted list.

2. In case no PKI public key technology is used to identify the trust service, a trust service is identified in the Qatar trusted list by means of an indicator expressed by a URI which uniquely and unambiguously identifies the trust service.

Annex II: Technical requirements for qualified trust service providers providing the remote creation as a service of qualified electronic signatures

II.1 General requirements

1. The qualified trust service provider providing the remote creation as a service of qualified electronic signatures as a qualified trust service shall conform to [ETSI TS 119 431-2] with the amendments specified in Annex I of these technical specifications with the additional amendments of the present Annex.

2. All references to ETSI EN 319 411-1 made directly or indirectly in [ETSI TS 119 431-2] shall be understood as referring to the version of that standard amended according to Annex IV of [TSP-CA] technical specifications.

II.2 Specific requirements for the creation of qualified electronic signatures based on X.509 certificates

1. Where the SCASC (Signature Creation Application Service Component) is used to create a qualified electronic signature, the signing qualified certificate shall identify the signatory.

2. The signing qualified certificate shall be contained in the created AdES signature.

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.
[TSP-CA]	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
[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.
[ETSI EN 319 102-1]	ETSI EN 319 102-1 V1.3.1 (2021-11): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
[ETSI EN 319 132-1]	ETSI EN 319 132-1 V1.2.1 (2022-02) : Electronic Signatures and Infrastructures (ESI) ; XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
[ETSI EN 319 142-1]	ETSI EN 319 142-1 V1.1.1 (2016-04) : Electronic Signatures and Infrastructures (ESI) ; PAdES digital signatures ; Part 1 : Building blocks and PAdES baseline signatures

[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 v1.3.1 (2023-10): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI TS 119 431-2]	ETSI TS 119 431-2 V1.2.1 (2023-06): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation
[ETSI TS 119 432]	ETSI TS 119 432 V1.2.1 (2020-10): Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation
[ETSI TS 119 612]	ETSI TS 119 612 v2.1.1 (2015-07): Electronic Signatures and Infrastructures (ESI); Trusted Lists
[CSC API]	Cloud Signature Consortium : Architectures and protocols for remote signature applications v2.0.0.2 (https://cloudsignatureconsortium.org/resources/)