Communications Regulatory Authority State of Qatar

هيئة تنظيم الاتصالات دولة قطر

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.

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to them in the Electronic Commerce and Transactions Law promulgated by Decree Law No. 16 of 2010 as amended or repealed and the Regulation of Certification Service Providers issued under the Communications Regulatory Authority President Decision No. [X] of 2024 (”CSPs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

Article 2: Provisions for trust service providers or qualified trust service providers and the trust service or qualified trust service

1. Pursuant to the "CSPs Regulation", trust service providers and the trust services they provide and qualified trust service providers and the qualified trust services they provide shall comply with the technical requirements laid down in Annex I hereto.

Annex I: Technical requirements for trust service providers or qualified trust service providers and the trust service or qualified trust service they provide

I.1 General requirements

1. The trust service provider or qualified trust service provider shall implement the recommendations of the CA/Browser Forum network security guide [CABF Network], items 1 to 4, where every occurrence of “CA system” shall be read as “trust service provider system” or as applicable “qualified trust service provider system” and where in item 4.c "CA/Browser Forum" is replaced by "the Authority".

2. The trust service provider or qualified trust service provider shall conform to [ETSI EN 319 401] with the amendments provided in the subsequent paragraphs of the present Article, which shall prevail over the corresponding requirements of the former.

3. All mentions of “trust service provider” in [ETSI EN 319 401] shall be understood as “trust service provider or qualified trust service provider as defined in the “CSPs Regulation””.

4. All mentions of “trust service” in [ETSI EN 319 401] shall be understood as “trust service or qualified trust service as defined in the “CSPs Regulation””.

5. REQ-5-04 of [ETSI EN 319 401] is amended so it reads:
“The risk assessment shall be regularly reviewed and revised:
    5.1 at least on a yearly basis; and
    5.2 at any change having an impact on the trust service provided, in particular when changing the provisions of the policies and/or practices statement set by the trust service provider as required by REQ-6.1-0.”

6. REQ-6.3-10 of [ETSI EN 319 401] is amended so it reads:
“The maximum interval between two checks shall be [one week] and shall be documented in the trust service practice statement.”

7. Regarding REQ-7.7-01 of [ETSI EN 319 401], requirements for the trustworthy systems managing certificates and time stamps shall be ensured by using systems conforming to [CEN TS 419 261] or any equivalent international standards.

I.2 Facility, Management, Operational and Security Controls

1. Any update to the risk assessment and mitigation plan shall be notified to the Authority together with the yearly notification of changes referred to in the section 4 “I.4 Notifications” of the present Annex.

2. The trust service provider or qualified trust service provider shall use all legal means it may need to verify the honesty of the personnel it uses for the provisioning of its trust service or qualified trust service, including outsourcers or subcontractors.

   In particular, the trust service provider or qualified trust service provider shall verify that it has not been established by a final judgement or a final administrative decision that a member of the personnel is guilty of an offense in contradiction with the tasks (s)he has been allocated by the trust service provider or qualified trust service provider. This includes being guilty of critical professional misconduct:

   2.1 by having violated applicable laws or regulations or ethical standards of the profession to which the person belongs, or

   2.2 by having engaged in any wrongful conduct which has an impact on its professional credibility where such conduct denotes wrongful intent or gross negligence. This includes fraud, significant deficiencies in performance of a contract, distortion of competition, and corruption.

3. The verifications in Paragraph **Error! Reference source not found.** of the present section shall be performed prior to the allocation of a trusted role and reviewed regularly, at least every two (2) years.

I.3 Cryptography and cryptographic suites

1. The trust service provider or qualified trust service provider shall use cryptographic suites in accordance with the recommendations provided in the latest version of the SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms of [SOG-IS Crypto WG].

2. The cryptographic suites and the cryptographic key lengths and parameters used by the trust service provider or qualified trust service provider shall be capable to resist to cryptographic attacks during the validity period of the data to which they are applied and, when applicable, of the associated certificate, whichever is the longer.

I.4 Notifications

1. On a yearly basis, the trust service provider or qualified trust service provider shall notify the Authority with an overview of all changes made to the provision of its trust service or qualified trust service having an impact on the statements made in the conformity assessment report.

I.5 Termination

1. When the trust service provider or qualified trust service provider notifies the Authority of its intention to cease operating as a trust service provider or qualified trust service provider or to cease the provision of a trust service or qualified trust service in line with Article 16.2.1 of the "CSPs Regulation", it shall include in the notification to the Authority a submission of an updated version of the trust service provider or qualified trust service provider termination plan.

2. The termination plan shall comply with the requirements of the section 6 "I.6 Structure and content of the termination plan of a trust service or qualified trust service provided by a trust service provider" of the present Annex in terms of format and content, particularly to cover the scheduled and unscheduled termination, partial or global termination.

3. The documentation associated to a trust service or qualified trust service termination plan shall include the following:
    a. Formal termination procedures;
    b. Formal termination procedures internal assessment, including regular internal assessment of the practical feasibility of the implementation of the termination plan;
    c. Formal termination procedures training;
    d. Formal termination procedures internal assessment reports;
    e. Formal termination procedures auditing reports;
    f. Formal termination (contractual) arrangements with third parties (incl. subcontractors, taking over parties, the Authority, etc.);
    g. Trust service or qualified trust service terms and conditions, practices and policy documents;

h. Up-to-date documentations for personal data protection rules compliancy:
   i) Treatment registers and data (and metadata) mapping;
   ii) Privacy impact assessments;
   iii) Documents (e.g., binding corporate rules) for particular cases of transfer outside Qatar;

i. As part of the risk management obligations from The Law:
   i) A termination-specific risk analysis shall be undertaken, documented and the associated mitigation measures shall be documented, and their implementation regularly controlled.
   ii) This analysis shall include a personal data impact assessment and documentation of the associated mitigation measures.

4. The revocation of the license, of a trust service provider or qualified trust service provider for the trust service or the qualified trust service it provides shall imply the immediate activation and execution of the termination plan for that trust service or qualified trust service and, when applicable, for the trust service provider or qualified trust service provider.

I.6 Structure and content of the termination plan of a trust service or qualified trust service provided by a trust service provider or qualified trust service provider

Front page

1. Document name & identification

   This clause shall include versioning, date of entering into force, status and document classification.

2. Trust service provider or qualified trust service provider (hereafter referred to as TSP for the remaining of this Annex) identification.

   This clause shall clearly identify the name of the TSP, and where applicable its registration number, as stated in the official records, its official postal address and its contact electronic address.

3. Identification of concerned trust service or qualified trust service (hereafter referred to as TS for the remaining of this Annex)

   This clause shall identify the TS covered by the termination plan.

Introduction

1. Overview

   This clause shall provide a general overview of the termination plan and a synopsis of the trust service provider or qualified trust service provider *and the trust service* or qualified trust service *it provides (hereafter referred to as TSP/TS) to which termination provisions apply.*

   A diagrammatic representation shall be provided.

   All participants and TS service components shall be identified.

2. Document name and identification rules

   This clause shall provide any applicable names or other identifiers for the termination plan document and for relevant referenced documents, when applicable.

3. TS to which the termination plan applies

   This clause shall provide a detailed identification of the TS to which termination provisions apply, in particular with regards to the Qatar trusted list service entry(ies) and the associated "Service digital identity" elements (i.e., public keys when based on public key infrastructure).

A diagram, or table representation, shall be provided.

4. Termination plan administration

   This clause shall provide the name and mailing address of the organization or authority that is responsible for the drafting, registering, maintaining, and updating of the termination plan.

   It shall identify the responsibilities and duties of that organization or authority with regards to the TSP/TS termination, termination plan reviewing, internal / external auditing processes, and its execution.

   This clause shall include the name, electronic mail address, and telephone number of a contact person, service or functional role.

5. Applicable national legislation and relevant provisions on TSP/TS termination

   This clause shall provide references to the applicable Qatar legislation and identify the relevant Qatar legal provisions on TSP/TS termination.

6. Definitions and abbreviations

   This clause shall contain a list of definitions for defined terms used within the document, as well as a list of abbreviations used in the document and their meanings.

Termination plan provisions

Scheduled termination

This clause shall describe the provisions and actions to be undertaken:

- In the context of the scheduled termination of part or of whole of the TS to which the termination plan applies; and/or
- In the context of the scheduled actions that could result in the partial or complete termination of the TS to which the termination plan applies.

The arranged/contracted custodian(s), insurers or 3rd parties involved in assisting the implementation of the termination shall be properly identified and their role and scope of assistance shall be clearly described.

The relevant actions and the associated provisions shall include, at least:

- Termination plan update and the provisions on its notification to the Authority.
- Identification of the operations to be ceased and the expected timing / scheduling.

- Identification of the operations to be ceased and the expected timing / scheduling.
- Identification of the expected impact on the relevant entries of the Qatar trusted list.
- Risk analysis update and updated mitigation measures.
- Identification of the financial resources and/or appropriate insurance to cover the costs required to properly execute the termination plan.
- Personal data impact assessment update and updated mitigation measures.
- Termination notifications and related actions:
  - Identification of the entities to be notified of the termination (e.g., the Authority, subscribers, relying parties, other TSP with which the terminated service has trust relationships, TSP staff and/or subcontractors).
  - For each notified entity or logical group of notified entities, specify the provisions on the termination notifications, the notification means and the expected timing/scheduling of those notifications.
  - Identification of the associated documentation.
  - Identification of the services whose termination is scheduled, the reason for such termination and the expected timing / scheduling.
  - Terms and conditions ruling the notified termination: This may include:
    - Arrangement(s) applicable with another TSP for the provision of future TS of similar nature.
    - Preservation of subscriber's related (personal) data.
    - Preservation of operational data and other relevant data to sustain the trustworthiness of the TS outputs and related evidences.
    - With regards to certificates, the conditions on their revocation (for unexpired and unrevoked certificates).
    - Foreseen compensations to subscribers, when applicable.
- Procedures for the execution of the termination actions.
- Identification of the personnel (staff and/or subcontractors), their requested expertise and training conditions.
- Transfer of recorded, auditing and archival records to the arranged / contracted custodian(s), and proper identification of custodian(s).

Unscheduled termination

This clause shall describe the provisions and actions to be undertaken:

- In the context of the unscheduled termination of part or of whole of the TS to which the termination plan applies; and/or
- In the context of unscheduled actions that could result in the partial or complete termination of the TS to which the termination plan applies.

Unexpected or unscheduled termination of the TSP/TS may result from different causes such as severe incident or disaster from which incomplete or unsatisfactory recovery could be reached, bankruptcy, court orders, and any unexpected reason forcing the TSP/TS to execute a termination.

This clause should address provisions and actions like those covered in the clause “Scheduled termination” above, considering the unexpected and unscheduled nature of the causes for termination and the potential significant decrease of delays within which those actions need to be undertaken.

The arranged/contracted custodian(s), insurers or 3rd parties involved in assisting the implementation of the unscheduled termination should be properly identified and their role and scope of assistance should be clearly described.

Internal/external compliance audit and other assessments

This clause shall address internal and external audit and other assessment, in particular:

- The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment.
- Frequency of compliance audit or other assessment.
- The identity and/or qualifications of the personnel performing the audit or other assessment.
- The relationship between the assessor and the TSP whose termination plan is being audited/assessed, including the degree of independence of the assessor.
- Actions taken as a result of deficiencies found during the termination plan audit or other assessment.
- Internal/external person(s) entitled to be communicated the results of an assessment, and/or the actions taken as a consequence.

Other provisions

This clause provides any other applicable provisions not fitting in with any of the above clause.

References

Reference	Title
[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 Network]	CA/Browser Forum: Network and certificate system security requirements
[ISO/IEC 27001]	ISO/IEC 27001:2022: Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements
[SOG-IS Crypto WG]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms (https://www.sogis.eu/uk/supporting_doc_en.html)