Communications Regulatory Authority State of Qatar | هيئة تنظيم الاتصالات دولة قطر

D4.4 QA-TSF-CRA Requirements on ad

Technical specifications and formats relating to the State of Qatar trusted list, adopted pursuant to Article 36.4 of the CSP Regulation

Version 1.0

25 February 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ascribed to them in the Electronic Commerce and Transactions Law promulgated by Decree Law No. 16 of 2010 as amended or repealed and the Regulation of Certification Service Providers issued under the Communications Regulatory Authority President Decision No. [X] of 2024, unless these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 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 on the Licensing and activities performed by Certification Service Providers issued under CRA President Decision No [X] 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”
“License”	An authorization issued pursuant to the provisions of

	"The Law" and the "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";

Article 2: Trusted list

1. Pursuant to Paragraph 4 of Article 36 of the "CSPs Regulation", the Authority shall establish, publish, and maintain a trusted list including information on the (qualified) trust service which they supervise, as well as information on the (qualified) trust services provided by them. This list shall comply with the technical specifications set out in Annex I and Article 3 of the present technical specifications.

Article 3: Trusted list signature

1. The Authority shall sign or seal electronically the trusted list in accordance with the technical specifications set out in Annex I.

2. For the signature or seal referred above, the Authority shall communicate publicly two or more scheme operator public key certificates, with shifted validity periods of at least 3 months, which correspond to the private keys that can be used to sign or seal electronically the trusted list when published.

Annex I:

Technical specifications for a common template for the Qatar trusted list

Chapter I

I.1 General requirements

The trusted list shall include both current and all historical information, dating from the inclusion of a (qualified) trust service provider in the trusted list, about the status of listed (qualified) trust services.

The information provided in the trusted list is primarily aimed at supporting the validation of (qualified) trust service tokens from (qualified) trust services, i.e. physical or binary (logical) objects generated or issued as a result of the use of a (qualified) trust service, e.g. namely (qualified) electronic signatures/seals, advanced electronic signatures/seals supported by a (qualified) certificate, qualified time stamps, etc.

I.2 Trusting the content of the Qatar trusted list

Prior to any interpretation of the Qatar trusted list, relying parties should:

- retrieve the trusted list from a secure location (hereafter 'TL-location'); and
- verify the authenticity and integrity of the trusted list. Especially, relying parties should verify the authenticity and integrity of the trusted list by verifying that it has been signed/sealed by one of the authorized certificates (hereafter the 'TL-signing certificates').

I.3 Pivot trusted list mechanism

First, the TL-location and TL-signing-certificates are published in the Official Gazette. Subsequent changes to the TL-location or TL-signing-certificates might, as a machine-processable approach, be published in the Qatar trusted list itself by the Authority. Such instance of the Qatar trusted list is hereafter referred to as a 'pivot TL', as it represents a pivot point in the historical values of the TL-location and the TL-signing certificates.

These pivot TLs form a chain of changes (changes of TL-location or TL-signing certificates) starting

from the initial situation published in the Official Gazette up to the current one. These pivot TLs are archived for later reference.

To conclude on the current list of TL-signing certificates in order to validate the signature of the TL as explained above, one shall reconstruct that chain of pivot TLs. How to reconstruct that chain is explained in the following paragraphs.

From a technical perspective, the TL-location, TL-signing certificates, and the location of archived pivot TLs are included in the Qatar trusted list such as:

- the `<OtherTSLPointer>` with QA `<SchemeTerritory>` contain the TL-location together with the PEM representation of the TL-signing certificates;
- the `<SchemeInformationURI>`, in reverse chronological order – that is, showing the most recent publication first – contains the list of:
    - zero or more URLs where the archived preceding pivot TLs are published, back until and followed by
    - the URL of the latest publication relevant to the Qatar trusted list in the Official Gazette.

In this respect, once the decision of the Authority to modify the TL-location or TL-signing certificates is reflected in a publication of a pivot TL, relying parties may detect these modifications in a machine processable way in the Qatar trusted list, namely from changes of:

- the `<OtherTSLPointer>` with QA `<SchemeTerritory>`;
- the `<SchemeInformationURI>`.

When verifying the authenticity and integrity of the Qatar trusted list, relying parties should, starting from the TL-location specified in the latest publication relevant to the Qatar trusted list in the Official Gazette, reconstruct the chain of pivot TLs to conclude on the current set of TL-signing certificates:

i. Based on the content of the Qatar trusted list published at the TL-location, retrieve the location(s) of all pivot TLs present in `<SchemeInformationURI>`;

ii. If no pivot TL is present, the current set of TL-signing certificates is the initial list in the above-mentioned publication of the Official Gazette;

iii. If pivot TLs are present: In the chronological order, for each pivot TL published at pivot TL location(s), verify the authenticity and integrity of the list; using:

   a. for the first pivot TL, the set of initial TL-signing certificates specified in the above-mentioned publication of the Official Gazette;

   b. for following pivot TLs, using the set of certificates specified in `<OtherTSLPointer>` with QA `<SchemeTerritory>` of the previous pivot TL in that ordered list; or

   c. The final result is the current set of TL-signing certificates.

I.4 Transition period observed by the Authority regarding the changes of TL-signing certificates or TL-location

After the publication of the pivot TL announcing changes in TL-signing certificates or TL-location, relying parties have 15 days (the duration of the transition period) to take these changes into account.

It is highly recommended to take these changes into account during the transition period rather than after it:

- During the transition period, this will have no impact on the ability to verify the authenticity and integrity of the Qatar trusted list, as the Authority will take the relevant measures (e.g. not using the newly-announced TL-signing certificates during the transition period, or publishing the TL at both locations during the transition period)
- After the transition period, this may have an impact on the ability to verify the authenticity and integrity of the Qatar trusted list, as the Authority may decide to:
  - Sign/seal the Qatar trusted list with one of the newly-announced TL-signing certificates.
  - Remove the Qatar trusted list from the previous TL-location.

Chapter II

II.1 Detailed specifications

The present specifications rely on the specifications and requirements set in ETSI TS 119 612 v2.1.1 (hereafter referred to as TS 119 612).

The present specifications rely on the requirements set in TS 119 612:

- When no specific requirements are set in the present specifications, requirements from TS 119 612 clauses 5 and 6, and Annex D shall apply in their entirety;
- When specific requirements are set in the present specifications, they shall prevail over the requirements for TS 119 612;
- In case of discrepancies between the requirements set in the present specifications and requirements from TS 119 612, the present specifications shall prevail.

References made in TS 119 612 to "advanced electronic signatures" (or “advanced electronic signatures under e-signature Directive”) and "advanced electronic seal" are replaced respectively by references to advanced electronic signatures and advanced electronic seals as defined in the “CSPs Regulation”.

References made in TS 119 612 to "qualified electronic signatures" and “qualified electronic seal" are replaced respectively by references to qualified electronic signatures and by qualified electronic seals as defined in the “CSPs Regulation”.

References made in TS 119 612 to "(EU) qualified certificates" (or “qualified certificate under e-signature Directive”) are replaced by references to qualified certificates as defined in the “CSPs Regulation”.

References made in TS 119 612 to a signatory, or a seal creator shall be references to the concepts as defined in the “CSPs Regulation”.

References made in TS 119 612 to a “TSP” shall be reference to the concepts of “Trust service provider” and when applicable “Qualified trust service provider” as defined in the “CSPs Regulation”.

References made in TS 119 612 to a “TS” shall be reference to the concepts of “Trust service” and when applicable “Qualified trust service” as defined in the “CSPs Regulation”.

References made in TS 119 612 to CA/QC are replaced by references to:

- /Q/CA/ForESignatures, /Q/CA/ForESeals

References made in TS 119 612 to CA/PKC are replaced by references to:

- nonQ/CA/ForESignatures, nonQ/CA/ForESeals and nonQ/CA/ForWebsiteAuthentication

II.2 TSL Type (clause 5.3.3)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.3 where, in the context of the Qatar trusted list, the URI shall be set to:

“http://cra.gov.qa/TrstSvc/TrustedList/TSLType/QAlist”.

II.3 Scheme name (clause 5.3.6)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.6 where, in the context of the Qatar trusted list, the English version shall be set to:

“QA: Trusted list of the State of Qatar including information related to the trust service providers and qualified trust service providers which are licensed within and supervised by the State, together with information related to the trust services and qualified trust services they provide, in accordance with the relevant provisions laid down in “The Law” and “CSPs Regulation” and technical specifications issued in implementation thereof.”

II.4 Scheme information URI (clause 5.3.7)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.7 where, in the context of the Qatar trusted list, the “appropriate information about the scheme” shall include as a minimum:

“The present list is the trusted list including information related to the trust service providers and the qualified trust service providers which are supervised by the Communications Regulatory Authority of the State of Qatar, together with information related to the trust services and the qualified trust services they provide, in accordance with the relevant provisions laid down in “The Law” and “CSPs Regulation” and technical specifications issued in implementation thereof”.

II.5 Status determination approach (clause 5.3.8)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.8 where, in the context of the Qatar trusted list, the URI shall be set to:

“http://cra.gov.qa/TrstSvc/TrustedList/StatusDetn/QAdetermination”.

The URI shall lead to the following text:

“Trust services listed in the Qatar trusted list have their status determined by or on behalf of the identified Scheme Operator under an appropriate system as defined by Qatar’s implementation of the applicable Qatar legislation and further described in the information pointed by the 'Scheme information URI' field of the Qatar trusted list.”

II.6 Scheme type/community/rules (clause 5.3.9)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.9 where, in the context of the Qatar trusted list, the URI shall be set to:

“http://cra.gov.qa/TrstSvc/TrustedList/schemerules/QA”.

The URI shall point towards the following descriptive text:

“*Policy/rules for the assessment of the listed services*

The State of Qatar supervises the (qualified) trust service providers established in its territory as laid down “The Law”, and “CSPs Regulation” and technical specifications issued in implementation thereof, to ensure that those (qualified) trust service providers and the (qualified) trust services they provide meet those requirements.

The State of Qatar trusted list includes, as a minimum, information specified in Article 36 of the “CSPs Regulation”.

The trusted list includes current and historical information about (qualified) trust services, notably on their licensed status (i.e. whether the trust service owns a license, either active or suspended).

The trusted list also provides information on the applicable supervisory scheme under which the (qualified) trust service providers and the (qualified) trust services they provide are listed.

Interpretation of the Trusted List

The general user guidelines for applications, services or products relying on a trusted list published in accordance with “The Law”, and “CSPs Regulation” and technical specifications issued in implementation thereof, are as follows:

The licensed status of a (qualified) trust service is indicated by the combination of:

- the “Service type identifier” (“Sti”) value in a service entry set to one of the types of (qualified) trust service, and
- the “Service current status” field value in that service entry set to “granted”,

as from the date indicated in the “Current status starting date and time”. When applicable, historical information about such licensed status is provided similarly.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures or qualified certificates for electronic seals:

A “Service type identifier” (“Sti”) entry with value:

- “/Q/CA/ForESignatures” (possibly further qualified as being a “Root-QCA” through the use of the appropriate “Service information extension” (“Sie”) “additionalServiceInformation Extension”) or
- “/Q/CA/ForESeals”

indicates that any end-entity certificate issued by or under the CA represented by the “Service digital identifier” (“Sdi”) CA’s public key and CA’s name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that:

- it includes the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1)
- it includes the id-etsi-qcs-QcType ETSI defined statement (id-etsi-qcs 6) matching the corresponding type:
    - id-etsi-qct-esign: certificate for electronic signatures
    - id-etsi-qct-eseal: certificate for electronic seals
- it includes the id-etsi-qcs-QcCCLegislation ETSI defined statement (id-etsi-qcs 7) with

value being “QA”

- and this is ensured by the Authority through a valid service status (i.e. “granted”) for that entry.

If an “Sie” “Qualifications Extension” information is present, then in addition to the above default rule, those certificates that are identified through the use of “Sie” “Qualifications Extension” information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status and/or the “QSCD support” (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific “Key usage” pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of “Qualifiers” used to compensate for the corresponding certificate content, and that are used respectively:

- to indicate the qualified certificate nature:
    - “QCStatement” meaning that all certificates identified by the applicable list of criteria are to be considered as qualified; and/or
    - “QCForESig” meaning that all certificates identified by the applicable list of criteria, when claimed or stated as qualified certificate(s), are qualified certificates for electronic signatures; or
    - “QCForESeal” meaning that all certificates identified by the applicable list of criteria, when claimed or stated as qualified certificate(s), are qualified certificates for electronic seals;
- to indicate that the certificate is not to be considered as qualified:
    - “NotQualified” meaning that all certificates identified by the applicable list of criteria are not to be considered as qualified; and/or
- to indicate the nature of the QSCD support:
    - “QCWithQSCD” meaning that all certificates identified by the applicable list of criteria, when claimed or stated as qualified, have their private key residing in a QSCD, or

- “QCNoQSCD” meaning that all certificates identified by the applicable list of criteria, when claimed or stated as qualified, have not their private key residing in a QSCD.

The information provided in the trusted list is to be considered as accurate meaning that:

- if the id-etsi-qcs 1 statement is not included in an end-entity certificate, and no “Sie” “Qualifications Extension” information is present for the corresponding service entry to qualify the certificate with a “QCStatement” qualifier; or
- if an “Sie” “Qualifications Extension” information is present for this service entry to qualify the certificate with a “NotQualified” qualifier; or
- “QCQSCDStatusAsInCert” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

then the certificate is not to be considered as qualified.

Regarding non-qualified trust service providers issuing non-qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

A “Service type identifier” (“Sti”) entry with value:

- “nonQ/CA/ForESignatures” or
- “nonQ/CA/ForESeals” or
- “nonQ/CA/ForWebSiteAuthentication”

indicates that any end-entity certificate issued by or under the CA represented by the “Service digital identifier” (“Sdi”) CA’s public key and CA’s name (both CA data to be considered as trust anchor input), is a non-qualified certificate (nonQC) provided that:

- it includes the id-etsi-qcs-QcType ETSI defined statement (id-etsi-qcs 6) with value being respectively for certificates for electronic signatures, for electronic seals or for website authentication:
  - id-etsi-qct-esign
  - id-etsi-qct-eseal
  - id-etsi-qct-web
- and this is ensured by the Supervisory Body through a valid service status (i.e. “granted”)

for that entry.

If an “Sie” “Non-qualifications Extension” information is present, then in addition to the above default rule, those certificates that are identified through the use of “Sie” “Non-qualifications Extension” information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated non-qualifiers providing additional information regarding their non-qualified status (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific “Key usage” pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These non-qualifiers are part of the following set of “Non-qualifiers” used to compensate for the corresponding certificate content, and that are used respectively:

- to indicate the non-qualified certificate nature:
    - “nonQCForESig” meaning that all certificates identified by the applicable list of criteria, when claimed or stated as non-qualified certificate(s), are non-qualified certificates for electronic signatures; or
    - “nonQCForESeal” meaning that all certificates identified by the applicable list of criteria, when claimed or stated as non-qualified certificate(s), are non-qualified certificates for electronic seals;
    - “nonQCForWSA” meaning that all certificates identified by the applicable list of criteria, when claimed or stated as non-qualified certificate(s), are non-qualified certificates for website authentication and code signing;
- to indicate that the certificate is not to be considered as non-qualified:
    - “NotNonQualified” meaning that all certificates identified by the applicable list of criteria are not to be considered as non-qualified.

“Service digital identifiers” are to be used as Trust Anchors in the context of validating electronic signatures or electronic seals for which the signer’s or seal creator’s certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate is representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other “Sti” type entry is that, for that “Sti” identified service type, the listed service named according to the “Service name” field value and uniquely identified by the “Service digital identity” field value has the current licensed status according to the “Service

current status" field value as from the date indicated in the "Current status starting date and time".

In addition, when the listed service has the licensed status and the "Sti" type entry has for value one of the URIs specified in section II.11.1 of the present annex, then the listed service has the corresponding qualified status starting from the date and time indicated in the indicated in the "Current status starting date and time".

Please refer to the applicable ""CSPs Regulation"" for further details on the fields, description and meaning for the State of Qatar trusted list."

II.7 TSL policy/legal notice (clause 5.3.11)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.11 where, in the context of the Qatar trusted list, this field shall include:

"The applicable legal framework for the present trusted list is the :The Law" and the ""CSPs Regulation"" and technical specifications issued in implementation thereof."

II.8 Pointers to other TSLs (clause 5.3.13)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.13 where, in the context of the Qatar trusted list, this field shall include a pointer towards itself, with content as published in the Official Gazette.

The referenced digital identities, validly representing the issuer(s) of the Qatar trusted list, shall be as published in the Official Gazette.

II.9 Next update (clause 5.3.15)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.15, except that in the context of the Qatar trusted list:

> The difference between the 'Next update' date and time and the 'List issue date and time' shall not exceed six (6) months.

II.10 Service type identifier (clause 5.5.1)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.5.1, except that, in the context of the Qatar trusted list, the quoted URI shall be:

- one of the URIs specified in section II.11.1 corresponding to the types of listed trust service entries for qualified trust services specified in ”The Law” and “CSPs Regulation; or
- one of the URIs specified in section II.12.1 corresponding to the types of listed trust services for non-qualified trust services specified in ”The Law” and “CSPs Regulation .

For clarity, the URIs for qualified trust services types or for types corresponding to components of qualified trust services begin with the string “http://cra.gov.qa/TrstSvc/Svctype/Q/” whereas the URIs for trust services types or types for components of trust services begin with the string “http://cra.gov.qa/TrstSvc/Svctype/nonQ/”.

II.11 Service types related to Qatar qualified trust services (clause 5.5.1.1)

II.11.1 Qatar qualified trust service types

(a)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/CA/ForESignatures
	Description: A qualified certificates for electronic signature issuing qualified trust service, creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services, and under which are provided the relevant and related revocation and certificate validity status information services (e.g., CRLs, OCSP responses) in accordance with ”The Law” and “CSPs Regulation”.
	Requirements: When the listed service is a “root” certificate generation service issuing certificates to one or more subordinates certificate generation services and from which a certification path can be established down to a certificate generation service issuing end-entity qualified certificates, this service type shall be further identified by using the “http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/Root-QCA” identifier (described in clause D.4) which is included in the additionalServiceInformation extension (clause 5.5.9.4) within a Service information extension (clause 5.5.9). When the certificate validity status information (e.g. CRLs, OCSP responses) related to the qualified certificates issued by the listed “/Q/CA/ForESignatures” identified service are not signed by the private key corresponding to the listed public key and when no certificate chain/path exists from the related certificate validity status information services (either CRL issuing entities or OCSP responders) to the listed “/Q/CA/ForESignatures” identified service public key, those certificate validity status

	information services shall be listed separately.

(b)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/CA/ForESeals
	Description: A qualified certificates for electronic seal issuing qualified trust service, creating and signing qualified certificates for electronic seals based on the identity and other attributes verified by the relevant registration services, and under which are provided the relevant and related revocation and certificate validity status information services (e.g., CRLs, OCSP responses) in accordance with ”The Law” and “CSPs Regulation”.
	Requirements: When the listed service is a “root” certificate generation service issuing certificates to one or more subordinates certificate generation services and from which a certification path can be established down to a certificate generation service issuing end-entity qualified certificates, this service type shall be further identified by using the “http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/Root-QCA” identifier (described in clause D.4) which is included in the additionalServiceInformation extension (clause 5.5.9.4) within a Service information extension (clause 5.5.9). When the certificate validity status information (e.g. CRLs, OCSP responses) related to the qualified certificates issued by the listed “/Q/CA/ForESeals” identified service are not signed by the private key corresponding to the listed public key and when no certificate chain/path exists from the related certificate validity status information services (either CRL issuing entities or OCSP responders) to the listed “/Q/CA/ForESeals” identified service public key, those certificate validity status information services shall be listed separately.

(c)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/TSA
	Description: A qualified time stamp issuing qualified trust service creating and signing qualified time stamps in accordance with ”The Law” and “CSPs Regulation”.

(d)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/EDS
	Description:

	A qualified electronic delivery service providing qualified electronic deliveries in accordance with ”The Law” and “CSPs Regulation”.

(e)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/PSES/ForQESignatures
	Description: A qualified preservation service for qualified electronic signatures in accordance with ”The Law” and “CSPs Regulation”.

(f)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/PSES/ForQESeals
	Description: A qualified preservation service for qualified electronic seals in accordance with ”The Law” and “CSPs Regulation”.

(g)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/QESValidation/ForQESignatures
	Description: A qualified validation service for qualified electronic signatures in accordance with ”The Law” and “CSPs Regulation”.

(h)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/QESValidation/ForQESeals
	Description: A qualified validation service for qualified electronic seals in accordance with ”The Law” and “CSPs Regulation”.

(i)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/RemoteQSigCDManagement
	Description: A management of remote qualified electronic signature creation device (QSigCD) qualified trust service which supports generation and management of signature creation data within QSigCD(s) on behalf and under control of remote signers, in accordance with ”The Law” and “CSPs Regulation”. This service is not PKI-based.

(j)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/RemoteQSealCDManagement
	Description: A management of remote qualified electronic seal creation device (QSealCD) qualified trust service which supports generation and management of seal creation data within QSealCD(s) on behalf and under control of remote seal creators, in accordance with ”The Law” and “CSPs Regulation”. This service is not PKI-based.

(k)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/Archiv
	Description: A qualified service for the archival of electronic data, in accordance with ”The Law” and “CSPs Regulation”.

(l)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/RemoteCreation/ForQESignatures
	Description: A qualified service for the remote creation of qualified electronic signatures, in accordance with ”The Law” and “CSPs Regulation”.

(m)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/RemoteCreation/ForQESeals
	Description: A qualified service for the remote creation of qualified electronic seals, in accordance with ”The Law” and “CSPs Regulation”.

(n)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/QSigCDProvision
	Description: A qualified service for the provision of qualified electronic signature creation devices, in accordance with ”The Law” and “CSPs Regulation”. This service is not PKI-based.

(o)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/QSealCDProvision
	Description:

	A qualified service for the provision of qualified electronic seal creation devices, in accordance with ”The Law” and “CSPs Regulation”. This service is not PKI-based.

II.11.2 Qatar qualified trust service component types

(a)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/Certstatus/OCSP
	Description: A certificate validity status information service issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a qualified trust service provider issuing qualified certificates, in accordance with ”The Law” and “CSPs Regulation”.

(b)	URI : http://cra.gov.qa/TrstSvc/Svctype/Q/Certstatus/CRL
	Description: A certificate validity status information services issuing and signing Certificate Revocation Lists (CRLs) and being part of a service from a qualified trust service provider issuing qualified certificates, in accordance with ”The Law” and “CSPs Regulation”.

II.12 Service types related to Qatar trust services (clause 5.5.1.2)

II.12.1 Qatar trust service types

(a)	URI : http://cra.gov.qa/TrstSvc/Svctype/nonQ/CA/ForESignatures
	Description: A certificate issuing trust service, creating and signing certificates for electronic signatures based on the identity and other attributes verified by the relevant registration services, and under which are provided the relevant and related revocation and certificate validity status information services (e.g., CRLs, OCSP responses) in accordance with ”The Law” and “CSPs Regulation”.
	Requirements:

	When the certificate validity status information (e.g. CRLs, OCSP responses) related to the certificates issued by the listed “nonQ/CA/ForESignatures” identified service are not signed by the private key corresponding to the listed public key and when no certificate chain/path exists from the related certificate validity status information services (either CRL issuing entities or OCSP responders) to the listed “nonQ/CA/ForESignatures” identified service public key, those certificate validity status information services shall be listed separately.

(b)	URI : http://cra.gov.qa/TrstSvc/Svctype/nonQ/CA/ForESeals
	Description: A certificate issuing trust service, creating and signing certificates for electronic seals based on the identity and other attributes verified by the relevant registration services, and under which are provided the relevant and related revocation and certificate validity status information services (e.g., CRLs, OCSP responses) in accordance with ”The Law” and “CSPs Regulation”.
	Requirements: When the certificate validity status information (e.g. CRLs, OCSP responses) related to the certificates issued by the listed “nonQ/CA/ForESeals” identified service are not signed by the private key corresponding to the listed public key and when no certificate chain/path exists from the related certificate validity status information services (either CRL issuing entities or OCSP responders) to the listed “nonQ/CA/ForESeals” identified service public key, those certificate validity status information services shall be listed separately.

(c)	URI : http://cra.gov.qa/TrstSvc/Svctype/nonQ/CA/ForWebsiteAuthentication
	Description: A certificate issuing trust service, creating and signing certificates for website authentication and code signing based on the identity and other attributes verified by the relevant registration services in accordance with ”The Law” and “CSPs Regulation”.
	Requirements: When the certificate validity status information (e.g. CRLs, OCSP responses) related

	to the qualified certificates issued by the listed “nonQ/CA/ForWebsiteAuthentication” identified service are not signed by the private key corresponding to the listed public key and when no certificate chain/path exists from the related certificate validity status information services (either CRL issuing entities or OCSP responders) to the listed “nonQ/CA/ForWebsiteAuthentication” identified service public key, those certificate validity status information services shall be listed separately.

(d)	URI : http://cra.gov.qa/TrstSvc/Svctype/nonQ/RemoteCreation/ForESignatures
	Description: A service for the remote creation of electronic signatures, in accordance with ”The Law” and “CSPs Regulation”.

(e)	URI : http://cra.gov.qa/TrstSvc/Svctype/nonQ/RemoteCreation/ForESeals
	Description: A service for the remote creation of electronic seals, in accordance with ”The Law” and “CSPs Regulation”.

II.12.2 Qatar trust service component types

(a)	URI : http://cra.gov.qa/TrstSvc/Svctype/nonQ/Certstatus/OCSP
	Description: A certificate validity status information service issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing certificates for electronic signatures or for electronic seals, in accordance with ”The Law” and “CSPs Regulation”.

(b)	URI : http://cra.gov.qa/TrstSvc/Svctype/nonQ/Certstatus/CRL
	Description: A certificate validity status information services issuing and signing Certificate Revocation Lists (CRLs) and being part of a service from a trust service provider issuing certificates for electronic signatures or for electronic seals, in accordance with ”The Law” and “CSPs Regulation”.

II.13 Service digital identity (clause 5.5.3)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.5.3 where, in the context of the Qatar trusted list, when the service type is "RemoteQSigCDManagement", "RemoteQSealCDManagement", "QSealCDProvision" or "QSigCDProvision", the value shall be an indicator expressed as a URI defined by the Authority in such a way that it identifies uniquely and unambiguously the service. The format of this URI shall be:

http://cra.gov.qa/TrstSvc/Svctype/Q/SERVICE_TYPE/Sdi/ID

where "SERVICE_TYPE" is one of the concerned service types (e.g. "RemoteQSigCDManagement") and "ID" is the unique identifier defined by the Authority. The content of the URI shall provide more information about the QSCD.

II.14 Service current status (clause 5.5.4)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.5.4 where, in the context of the Qatar trusted list, the identifier of the status of the services of a type specified in section II.11.1 or II.12.1 shall be either:

- "http://cra.gov.qa/TrstSvc/TrustedList/Svcstatus/granted" when the (qualified) trust service to which it relates is licensed (and qualified when the Sti is part of the section II.11.1); or
- "http://cra.gov.qa/TrstSvc/TrustedList/Svcstatus/withdrawn" when the (qualified) trust service to which it relates is not licensed (and no longer qualified when the Sti is part of the section II.11.1).

In the case of a trust service component type, or a qualified trust service component type, the same status URIs apply and mean that the corresponding service component is part of the provision of a licensed trust service (for URIs defined in II.12.2) or of a qualified trust service (for URIs defined in II.11.2).

II.15 expiredCertsRevocationInfo extension (clause 5.5.9.1)

This field is optional and may only be present when used with the following 'Service types' (clause 5.5.1):

- "http://cra.gov.qa/TrstSvc/Svctype/Q/CA/ForESignatures";
- "http://cra.gov.qa/TrstSvc/Svctype/Q/CA/ForESeals";
- "http://cra.gov.qa/TrstSvc/Svctype/Q/Certstatus/OCSP";

- “http://cra.gov.qa/TrstSvc/Svctype/Q/Certstatus/CRL”;
- “http://cra.gov.qa/TrstSvc/Svctype/nonQ/CA/ForESignatures”;
- “http://cra.gov.qa/TrstSvc/Svctype/nonQ/CA/ForESeals”;
- “http://cra.gov.qa/TrstSvc/Svctype/nonQ/CA/ForWebsiteAuthentication”;
- “http://cra.gov.qa/TrstSvc/Svctype/nonQ/Certstatus/OCSP”;
- “http://cra.gov.qa/TrstSvc/Svctype/nonQ/Certstatus/CRL”.

II.16 Qualifications extension (clause 5.5.9.2)

In the context of the Qatar trusted list, this field shall comply with the requirements of clause 5.5.9.2.0 of TS 119 612 amended so that:

i. “trust service of type “CA/QC”” shall read “trust service of type “/Q/CA”;
ii. “an SSCD or in a QSCD” shall read “a QSCD”; and
iii. The list of “qualifiers” referred to in clause 5.5.9.2.1 of TS 119 612 “QualificationElement” shall refer to the qualifiers defined in clause 5.5.9.2.3 of the present document.

II.17 Qualifier (clause 5.5.9.2.3)

In the context of the Qatar trusted list, the following qualifiers are defined. They shall only be used when the type of service to which it applies is "/Q/CA".

- QCWithQSCD: As defined in TS 119 612 clause 5.5.9.2.3 but with URI being adjusted to "http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD”;
- QCNoQSCD: As defined in TS 119 612 clause 5.5.9.2.3 but with URI being adjusted to "http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD”;
- QCQSCDStatusAsInCert: As defined in TS 119 612 clause 5.5.9.2.3 but with URI being adjusted to "http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/QCQSCDStatusAsInCert”;
- QCForESig: As defined in TS 119 612 clause 5.5.9.2.3 but with URI being adjusted to "http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/QCForESig";
- QCForESeal: As defined in TS 119 612 clause 5.5.9.2.3 but with URI being adjusted to "http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/QCForESeal";
- NotQualified: As defined in TS 119 612 clause 5.5.9.2.3 but with URI being adjusted to "http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/NotQualified";
- QCStatement: As defined in TS 119 612 clause 5.5.9.2.3 but with URI being adjusted to

"http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/QCStatement".

Regarding the caution to be taken with the use of the “QCStatement” qualifier, the statement in TS 119 612 clause 5.5.9.2.3 is replaced by:

The QCStatement qualifier shall be used with extreme caution by TLSOs when and only when strong evidence exists that certificates identified through the applied filters are indeed to be considered as qualified certificates.

II.18 additionalServiceInformation extension (clause 5.5.9.4)

This field is optional and shall comply with the specifications from TS 119 612 clause 5.5.9, except that URIs defined under (a)i, (a)ii, and (a)iii are not applicable in the Qatar trusted list context, and under (a)iv “RootCA-QC” shall read “Root-QCA”.

II.20 Non-qualifications Extensions

Note: This section is not defined in TS 119 612.

This field shall be present when the information present in the non-qualified certificates created and signed by or under a listed trust service of the type “nonQ/CA” does not allow machine-processable identification:

- of the fact that it is not a non-qualified certificate; and/or
- whether the certificate has been issued for electronic signatures, for electronic seals or for web site authentication.

This field shall comply with clause 5.5.9.2 of TS 119 612, with the following changes:

- “qualification” is replaced by “non-qualification”; and
- “QualificationElement” is replaced “NonQualificationElement”; and
- “qualifier” field is replaced by a “non-qualifier” field with the following indicators expressed as URIs:
    - “http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/non-QCForESig”: to indicate that all certificates identified by the applicable list of criteria, when they are claimed or stated as being non-qualified, are issued for electronic signatures;
    - “http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/non-QCForESeal”: to indicate that all certificates identified by the applicable list of criteria, when they are claimed or stated as being non-qualified, are issued for electronic seals;

- “http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/non-QCForWSA”: to indicate that all certificates identified by the applicable list of criteria, when they are claimed or stated as being non-qualified, are issued for web site authentication;
- “http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/NotNonQualified”: to indicate that all certificates identified by the applicable list of criteria are not to be considered as non-qualified certificates.

II.21 TL publication (clause 6.1)

TLSO does not publish a digest that is computed as the SHA-256 hash value of the binary representation of the trusted list, at the URI that ends with “. sha2” as described in clause 6.1 of ETSI TS 119 612.

II.22 Common trusted lists URIs (clause D.4)

The following URI is registered in the State of Qatar:

- “http://cra.gov.qa/TrstSvc/TrustedList/SvcInfoExt/Root-QCA” (as Service information extensions/additionalServiceInformation Extension/): A Root Certification Authority from which a certification path can be established down to a Certification Authority issuing qualified certificates. This value shall not be used if the service type is not “http://cra.gov.qa/TrstSvc/Svctype/Q/CA/ForESignatures”, “http://cra.gov.qa/TrstSvc/Svctype/Q/CA/ForESeals”.

II.23 Service current and previous statuses (clause D.5.6)

The following URIs are registered in the State of Qatar:

- “http://cra.gov.qa/TrstSvc/TrustedList/Svcstatus/granted” (granted): Following pre-authorization and active approval activities, in compliance with the provisions laid down in ”The Law” and “CSPs Regulation”, it indicates that the Authority identified in the "Scheme operator name" (clause 5.3.4) has granted a “licensed” status, and when applicable a “qualified” status when the “Service type URI” is of a qualified trust service type, to the corresponding (qualified) trust service being of a service type specified in clause 5.5.1 and identified in "Service digital identity" (see clause 5.5.3), and to the (qualified) trust service provider identified in "TSP name" (see clause 5.4.1) for the provision of that service.

- “http://cra.gov.qa/TrstSvc/TrustedList/Svcstatus/withdrawn” (withdrawn): In compliance with

the provisions laid down in ”The Law” and “CSPs Regulation”, it indicates that the “licensed” status, and when applicable the “qualified” status when “Service type URI” is of a qualified trust service type, have not been initially granted or have been revoked/withdrawn by the Authority from the (qualified) trust service being of a service type specified in clause 5.5.1 and identified in "Service digital identity" (see clause 5.5.3), and from its (qualified) trust service provider identified in "TSP name" (see clause 5.4.1) for the provision of that service.

References

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