قرار رقم (54) لسنة 2023م
بشأن
اعتماد الصيغ والمواصفات الفنية الخاصة بقائمة الثقة الإماراتية

رئيس مجلس إدارة الهيئة العامة لتنظيم قطاع الاتصالات والحكومة الرقمية،،،،

بعد الاطلاع على المرسوم بقانون اتحادي رقم (3) لسنة 2003 في شأن تنظيم قطاع الاتصالات ولائحته التنفيذية وتعديلاتهما،

وعلى المرسوم بقانون اتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة ولائحته التنفيذية،

وبناءً على ما عرضه مدير عام الهيئة العامة لتنظيم قطاع الاتصالات والحكومة الرقمية، وموافقة مجلس إدارة الهيئة في اجتماعه المنعقد بتاريخ 18 ديسمبر 2023م، وعلى مذكرة الموافقة المرفوعة إليه من إدارة الهيئة،

قررنا ما يلي:

المادة (١)

يُعتمد بموجب هذا القرار "الصيغ والمواصفات الفنية الخاصة بقائمة الثقة الإماراتية" المُرفقة بهذا القرار.

المادة (٢)

يُعمل بهذا القرار اعتباراً من تاريخ صدوره، ويُنشر في الجريدة الرسمية.

صدر بتاريخ 18 ديسمبر 2023م.

The technical specifications and formats relating to the United Arab Emirates trusted list

Issue Date: 18 Dec.2023

Telecommunications and Digital Government Regulatory Authority (TDRA)
P O Box 26662, Abu Dhabi, United Arab Emirates (UAE)
www.tdra.gov.ae

Article (1)

Definitions

The terms, words, and phrases used in this Resolution shall have the same meaning as are ascribed to them in the Federal Decree Law No. (46) of 2021 On Electronic Transactions and Trust Services unless this Resolution expressly provides for otherwise, or the context in which those terms, words and phrases are used in this Resolution requires otherwise. For the purposes of this Resolution, the following terms and words shall have the meanings ascribed to them below:

"UAE" United Arab Emirates;

"The Authority" the Telecommunications and Digital Government Regulatory Authority ("the TDRA");

"Scheme operator" authority in charge of establishing, publishing and maintaining a trusted list;

"UAE trusted list" trusted list as defined in Federal Decree Law No. (46) of 2021.

Article (2)

Trusted list

1. Pursuant to Article 34(1) of the Executive Regulation No. (28) of 2023, the Authority shall establish, publish and maintain a trusted list including information on the trust service providers, which they supervise, as well as information on the trust services provided by them. This list shall comply with the technical specifications set out in Annexure I.

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 Annexure 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.

Article (4)

Trust service digital identity

1. Pursuant to Article 34(5) of the Executive Regulation No. (28) of 2023, when adding new trust service providers to the list the Authority shall connect each trust service provided with a digital identifier to allow to identify the service licensed in a unique way. Licensed trust services listed in the trusted list shall be uniquely and unambiguously identified in compliance with the technical specifications laid down in Annexure I.

Annexure I

TECHNICAL SPECIFICATIONS FOR A COMMON TEMPLATE FOR UAE TRUSTED LIST

Chapter I

General requirements

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

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

Trusting the content of UAE trusted list

Prior to any interpretation of the UAE 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') (note: more precisely, signed/sealed by the corresponding private key).

Pivot TL mechanism

Initially, the TL-location and TL-signing certificates are specified in the Official Gazette. Later, following the decision of TDRA to modify the TL-location or the set of TL-signing certificates, TDRA might, as a machine-processable approach, publish these modifications in the UAE trusted list itself. Such an instance of the 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 UAE trusted list such as:

- the `<OtherTSLPointer>` with AE `<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 UAE trusted list in the Official Gazette.

In this respect, once the decision of TDRA 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 UAE trusted list, namely from changes of:

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

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

1. Based on the content of the UAE TL published at the TL-location, retrieve the location(s) of all pivot TLs present in `<SchemeInformationURI>`;
2. 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
3. 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; or
   b. for following pivot TLs, using the set of certificates specified in `<OtherTSLPointer>` with AE `<SchemeTerritory>` of the previous pivot TL in that ordered list;
   c. The final result is the **current set of TL-signing certificates**.

Transition period observed by TDRA 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 UAE trusted list, as TDRA 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 UAE trusted list, as TDRA may decide to:
  - Sign/seal the UAE trusted list with one of the newly-announced TL-signing certificates.
  - Remove the UAE trusted list from the previous TL-location.

Interpretation of the content of a UAE trusted list

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Federal Decree Law No. (46) of 2021 are as follows:

The "licensed" status of a 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 trust services;
- 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". Historical information about such a "licensed" status is similarly provided when applicable.

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

A "Service type identifier" ("Sti") entry with value:

- "Q/CA/ForeSignatures" (possibly further qualified as being a "RootQCA" 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 "AE"
- and this is ensured by the Supervisory Body 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 (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

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-qcs-esign
  - id-etsi-qcs-eseal
  - id-etsi-qcs-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 electronic seals;
- 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 seals for which 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 qualified or approval status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time".

Please refer to the Executive Regulation No. (28) of 2023 for further details on the fields, description and meaning for the UAE trusted list.'

Chapter II

Detailed specifications for the common template for the trusted list

The specifications for the UAE trusted list rely on the specifications and requirements set in ETSI TS 119 612 v2.2.1 (hereinafter referred to as TS 119 612[1]).

The following specific requirements overrule the requirements from TS 119 612 meaning that:

- When no specific requirements are set in the UAE Regulation, requirements from TS 119 612 clauses 5 and 6, and Annex D shall apply in their entirety;
- When specific requirements are set in the UAE Regulation, they shall prevail over the requirements for TS 119 612;
- In case of discrepancies between the requirements set in the UAE Regulation and requirements from TS 119 612, UAE Regulation requirements 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 trusted electronic signatures and to trusted electronic seals as defined in Federal Decree Law No. (46) of 2021.

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 Federal Decree Law No. (46) of 2021.

[1] ETSI TS 119 612 V2.2.1(2016-04): Electronic Signatures and Infrastructures (ESI); Trusted lists;

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 Federal Decree Law No. (46) of 2021.

References made in TS 119 612 to a signatory or a seal creator shall be references to the concepts as defined in Federal Decree Law No. (46) of 2021.

References made in TS 119 612 to a (Q)TSP or a (Q)TS shall be references to the concepts as defined in Federal Decree Law No. (46) of 2021.

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

- Q/CA/ForeSignatures, Q/CA/ForeSeals
- nonQ/CA/ForeSignatures, nonQ/CA/ForeSeals, and nonQ/CA/ForWebsiteAuthentication

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 UAE trusted list, the URI shall be set to:

- “http://uri.trustservices.gov.ae/TrstSvc/TrustedList/TSLType/AElist”.

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 UAE trusted list, the URI shall be set to:

- “http://uri.trustservices.gov.ae/TrstSvc/TrustedList/StatusDetn/AEdetermination” .

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 UAE trusted list, the URI shall be set to:

- “http://uri.trustservices.gov.ae/TrstSvc/TrustedList/schemerules/AEcommon”.

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 UAE trusted list, this field shall include a pointer towards itself, with content as published in the UAE Official Gazette.

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

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 UAE trusted list:

- The difference between the 'Next update' date and time and the 'List issue date and time' shall not exceed one (1) year.

TSP trade name (clause 5.4.2)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.4.2, except that, in the context of UAE trusted list:

- When the TSP is a legal person, the identifier shall be expressed using the following structure for the corresponding character string in the presented order:
    a) “NTRAE”; and
    b) hyphen-minus “-“(Ox2D (ASCII), U+002D (UTF-8)); and

c) 2 characters identifying the authority code; and
d) full stop ".“(Ox2E (ASCII), U+002E (UTF-8)); and
e) identifier assigned to the TSP by the authority above.

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.

The quoted URI shall be:

a) one of the URIs specified in clause 5.5.1.1 corresponding to the types of listed trust services for qualified trust services specified in Federal Decree Law No. (46) of 2021; or
b) one of the URIs specified in clause 5.5.1.2 corresponding to the types of listed trust services for non-qualified trust services specified in Federal Decree Law No. (46) of 2021.

UAE Regulation qualified trust service types (clause 5.5.1.1)

(a)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/CA/ForeSignatures
	Description: A qualified certificate for electronic signatures issuing 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 Federal Decree Law No. (46) of 2021.
	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://uri.trustservices.gov.ae/TrstSvc/TrustedList/SvcInfoExt/RootQCA" 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. When the management of the electronic signature creation data on behalf of the signatory for qualified electronic signatures is performed by a QTSP, then the qualified certificates for which the private key resides in such a device shall be further identified and specified through the use of a Qualifications extension (clause 5.5.9.2) within a Service information extension (clause 5.5.9) by using the appropriate criteria and qualifiers (clause 5.5.9.2.3).

(b)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/CA/ForeSeals
	Description: A qualified certificate for electronic seals issuing 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 Federal Decree Law No. (46) of 2021.
	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://uri.trustservices.gov.ae/TrstSvc/TrustedList/SvcInfoExt/RootQCA" 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 sealed 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. When the management of the electronic seal creation data on behalf of the signatory for qualified electronic seals is performed by a QTSP, then the qualified certificates for which the private key resides in such a device shall be further identified and specified through the use of a Qualifications extension (clause 5.5.9.2) within a Service information extension (clause 5.5.9) by using the appropriate criteria and qualifiers (clause 5.5.9.2.3).

(c)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/Certstatus/OSCP
	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.

(d)	URI: http://uri.trustservices.gov.ae/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.

(e)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/TSA
	Description: A qualified electronic time stamp generation service creating and signing qualified electronic time stamps in accordance with Federal Decree Law No. (46) of 2021.

(f)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/EDS
	Description: A qualified electronic delivery service providing qualified electronic deliveries in accordance with Federal Decree Law No. (46) of 2021.

(g)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/PSQES/ForeSignatures
	Description: A qualified preservation service for qualified electronic signatures in accordance with Federal Decree Law No. (46) of 2021.

(h)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/PSQES/ForeSeals
	Description: A qualified preservation service for qualified electronic seals in accordance with Federal Decree Law No. (46) of 2021.

(i)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/QESValidation/ForeSignatures
	Description: A qualified validation service for qualified electronic signatures in accordance with Federal Decree Law No. (46) of 2021.

(j)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/QESValidation/ForeSeals
	Description: A qualified validation service for qualified electronic seals in accordance with Federal Decree Law No. (46) of 2021.

(k)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/RemoteQSigCDManagement
	Description: A qualified service for remote QSigCD (qualified electronic signature creation device) management which supports generation and management of signature creation data within QSigCD(s) on behalf and under control of remote signers, in accordance with Federal Decree Law No. (46) of 2021. This service is not PKI-based.

(l)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/RemoteQSealCDManagement
	Description: A qualified service for remote QSealCD (qualified electronic seal creation device) management which supports generation and management of signature creation data within QSealCD(s) on behalf and under control of remote seal creators, in accordance with Federal Decree Law No. (46) of 2021. This service is not PKI-based.

(m)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/LocalQSigCDProvision
	Description: A qualified service for the issuance of qualified signature creation devices, in accordance with Federal Decree Law No. (46) of 2021. This service is not PKI-based.

(n)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/LocalQSealCDProvision
	Description: A qualified service for the issuance of qualified seal creation devices, in accordance with Federal Decree Law No. (46) of 2021. This service is not PKI-based.

UAE Regulation non-qualified trust service types (clause 5.5.1.2)

(a)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/CA/ForeSignatures
	Description: A certificate for electronic signatures generation service, not qualified, creating and signing non-qualified public key certificates based on the identity and other

	attributes verified by the relevant registration services, in accordance with Federal Decree Law No. (46) of 2021.
	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 is 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://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/CA/ForeSeals
	Description: A certificate for electronic seals generation service, not qualified, creating and signing non-qualified public key certificates based on the identity and other attributes verified by the relevant registration services, in accordance with Federal Decree Law No. (46) of 2021.
	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 is 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://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/CA/ForWebSiteAuthentication
	Description: A certificate for website authentication generation service, not qualified, creating and signing non-qualified public key certificates based on the identity and other attributes verified by the relevant registration services, in accordance with Federal Decree Law No. (46) of 2021.
	Requirements: When the certificate validity status information (e.g. CRLs, OCSP responses) related to the certificates issued by the listed "nonQ/CA/ForWebSiteAuthentication" identified service is 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://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/Certstatus/OCSP
	Description: A certificate validity status service, not qualified, issuing Online Certificate Status Protocol (OCSP) signed responses.

(e)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/Certstatus/CRL
	Description: A certificate validity status service, not qualified, issuing CRLs.

(f)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/ESigCreation
	Description: A (remote) creation of electronic signatures service, not qualified, in accordance with Federal Decree Law No. (46) of 2021.

(g)	URI: http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/ESealCreation
	Description: A (remote) creation of electronic seals service, not qualified, in accordance with Federal Decree Law No. (46) of 2021.

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 UAE trusted list, when the service type is “RemoteQSigCDManagement”, “RemoteQSealCDManagement”, “LocalQSigCDProvision” or “LocalQSealCDProvision”, the value shall be an indicator expressed as a URI defined by TDRA in such a way that it identifies uniquely and unambiguously the service. The format of this URI shall be:

- http://uri.trustservices.gov.ae/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 TDRA. The content of the URI shall provide more information about the QSCD.

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 UAE trusted list:

- The identifier of the status of the services of a type specified in clause 5.5.1.1 or in 5.5.1.2 shall be either "http://uri.trustservices.gov.ae/TrstSvc/TrustedList/Svcstatus/granted" or "http://uri.trustservices.gov.ae/TrstSvc/TrustedList/Svcstatus/withdrawn”.

expiredCertsRevocationInfo Extension (clause 5.5.9.1)

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

- “http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/CA/ForeSignatures”;
- “http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/CA/ForeSeals”;
- “http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/Certstatus/OSCP”;
- “http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/Certstatus/CRL”;

- “http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/CA/ForeSignatures”;
- “http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/CA/ForeSeals”;
- “http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/CA/ForWebSiteAuthentication”;
- “http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/Certstatus/OCSP”;
- “http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/Certstatus/CRL”.

Qualifier (clause 5.5.9.2.3)

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

- "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD” as defined in TS 119 612 clause 5.5.9.2.3;
- "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD” as defined in TS 119 612 clause 5.5.9.2.3;

- QCForESig as defined in TS 119 612 clause 5.5.9.2.3 but with URI radix being adjusted to "http://uri.trustservices.gov.ae/TrstSvc/TrustedList/SvcInfoExt/QCForESig";
- QCForESeal as defined in TS 119 612 clause 5.5.9.2.3 but with URI radix being adjusted to "http://uri.trustservices.gov.ae/TrstSvc/TrustedList/SvcInfoExt/QCForESeal";

- NotQualified as defined in TS 119 612 clause 5.5.9.2.3 but with URI radix being adjusted to "http://uri.trustservices.gov.ae/TrstSvc/TrustedList/SvcInfoExt/NotQualified";

- QCStatement as defined in TS 119 612 clause 5.5.9.2.3 but with URI radix being adjusted to "http://uri.trustservices.gov.ae/TrstSvc/TrustedList/SvcInfoExt/QCStatement".

Regarding the caution to be observed 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.

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 UAE context.

Non-qualifications Extensions (clause 5.5.9.5)

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://uri.trustservices.gov.ae/TrstSvc/TrustedLists/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://uri.trustservices.gov.ae/TrstSvc/TrustedLists/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://uri.trustservices.gov.ae/TrstSvc/TrustedLists/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://uri.trustservices.gov.ae/TrstSvc/TrustedLists/SvcInfoExt/NotNon Qualified": to indicate that all certificates identified by the applicable list of criteria are not to be considered as non-qualified certificates.

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.

Common trusted lists URIs (clause D.4)

The following URI is registered in UAE:

- "http://uri.trustservices.gov.ae/TrstSvc/TrustedList/SvcInfoExt/RootQCA" (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://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/CA/ForeSignatures", "http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/CA/ForeSeals".

Service current and previous statuses (clause D.5.6)

The following URIs are registered in UAE:

- “http://uri.trustservices.gov.ae/TrstSvc/TrustedList/Svcstatus/granted” (**granted**): Following pre-authorization and active approval activities, in compliance with the provisions laid down in with Federal Decree Law No. (46) of 2021 , it indicates that the Supervisory Body identified in the "Scheme operator name" (see clause 5.3.4) has granted a “licensed” status to the corresponding 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 trust service provider identified in "TSP name" (see clause 5.4.1) for the provision of that service;

- “http://uri.trustservices.gov.ae/TrstSvc/TrustedList/Svcstatus/withdrawn” (**withdrawn**): In compliance with the provisions laid down in Federal Decree Law No. (46) of 2021 , it indicates that the “license” status has not been initially granted or have been withdrawn by the Supervisory Body from the 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 trust service provider identified in "TSP name" (see clause 5.4.1) for the provision of that service.