Telecommunications And Digital Government Regulatory Authority

TSP Framework

TL Guidelines for relying parties

Issue date: 19/March/2024

Revision history

Version	Date	Description
1.0	19 March 2024	First version release

References

Reference	Title
[EN 319 412-5]	ETSI EN 319 412-5 V2.4.1(2023-09): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[Law (1)]	Federal Law No. (1) of 2006 On Electronic Commerce and Transactions
[Law (46) 2021]	Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services Version 20.09.2021 https://u.ae/en/about-the-uae/digital-uae/electronic-transactions-and-trust-services-law
[TDRA TL Resolution]	The technical specifications and formats relating to the United Arab Emirates trusted list. Issue date : 18.12.2023
[Reg (28) 2023]	Federal Executive Regulation No. (28) of 2023
[TS 119 172-4]	ETSI TS 119 172-4 V1.1.1(2021-05): Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists
[TS 119 612]	ETSI TS 119 612 v2.2.1 (2016-04): Electronic Signatures and Infrastructures (ESI); Trusted Lists
[TS 119 615]	ETSI TS 119 615 V1.2.1(2023-06): Electronic Signatures and Infrastructures (ESI); Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists
[RFC 3161]	IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" https://datatracker.ietf.org/doc/rfc3161/
[RFC 5280]	IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" https://datatracker.ietf.org/doc/html/rfc5280
[EN 319 412-5]	ETSI EN 319 412-5 V2.4.1(2023-09): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[TR 119 001]	ETSI TR 119 001 V1.2.1 (2016-03): Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations
[EN 319 102-1]	ETSI EN 319 102-1 V1.3.1 (2021-11): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

Table of Contents

1. Introduction

The present document (and corresponding algorithm) is based on the Digital Europe's eSignature Building Block's document available at https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Qualified+electronic+signature+-+QES+validation+algorithm and adapted to the UAE context.

It aims at providing guidelines for the validation of qualified and advanced electronic signatures and seals based on the content of the national trusted list.

Compared to the Digital Europe's document for EU, the main adaptation for UAE are:

- Both qualified and non-qualified trust services are licensed trust services. Withdrawing the license of a qualified trust service doesn't make it non-qualified but not licensed (it shall stop offering the service).
- Consequently, non-qualified extensions are necessary, as a counterpart of qualified extensions, to compensate for the lack of standardized machine-processable information in the certificate content.
- Both qualified and non-qualified trust services are included in the trusted list.
- QcCompliance shall be understood in the context of UAE, that is together with a QcCClegislation = "AE".
- The QcType statement shall be present in both qualified and non-qualified certificates (i.e. issued by (qualified) trust services providers licensed for the issuance of (qualified) certificates).
- There is no QWAC definition in UAE legal framework.

This algorithm should not be considered as a standard but rather as guidelines for implementers, or parties interested in understanding how electronic signatures validation can be implemented.

Two ETSI standards, [TS 119 615] and [TS 119 172-4] standardize "Procedures for using and interpreting European Union Member States national trusted lists" and "Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists". These 2 standards shall be adapted to the UAE context according to the guidelines provided in the present document.

The algorithm below focuses on determining 3 sub-conclusions:

- Whether the certificate is qualified, non-qualified, or not licensed;
- What is the type of this certificate;
- Whether the corresponding private key is protected by a QSCD.

These sub-conclusions are important for handling the requirements of Article 20 of [Law (46) of 2021] on qualified electronic signatures and seals validation. The aim of the algorithm is more generally to determine whether an electronic signature or seal can be considered as QESig / QESeal / AdESig-QC / AdESeal-QC / AdESig-nonQC / AdESeal-nonQC / AdES-notLicensed / Indeterminate cases by interpreting content present in the national trusted list and in the signing / sealing certificate.

Please note, however, that verifying compliance against requirements for advanced electronic signatures and advanced electronic seals (e.g. requirements on the signature / seal format, cryptographic requirements) are outside of the scope of the present document.

The algorithm focuses on the case where the time of signing is after the entry into force of the [Law (46) of 2021]. Please note that this time of signing is the “best possible time”, for which a proof of existence is available. By default, it is the validation time (current time). If any proof of the existence of a signature is found, the lowest trusted time is used (signature-timestamp).

2. Definitions and abbreviations

These definitions and abbreviations are based on [TR 119 001] and [EN 319 102-1], adapted to the UAE context.

2.1 General definitions and abbreviations

1. QC: qualified certificate.
2. nonQC: certificate issued by a TSP licensed for the issuance of non-qualified certificates. If a certificate is neither QC nor nonQC, it is said to be non-licensed in the present context (i.e. it is not issued by a TSP licensed for the issuance of (non-)qualified certificates).
3. SB: Supervisory Body.
4. sigCert: signing certificate. The certificate corresponding to the private key that was used to produce a digital signature.
5. TL: trusted list.
6. Qualified status of a certificate: whether the certificate is qualified or not. By extension, whether the certificate is non-qualified or not.
7. TS: trust service
8. TSP: trust service provider.
9. Type of QC: type of a qualified certificate. Two types are defined by the [Law (46) of 2021]: for electronic signature, for electronic seal.
10. Type of nonQC: type of a non-qualified certificate. Three types are defined by the [Law (46) of 2021]: for electronic signature, for electronic seal, for website authentication.
11. WSA: website authentication (term used to describe a type of certificate, i.e. certificate for WSA).

2.2 Definitions and abbreviations regarding signature levels

1. AdES: digital signature that is either under CAdES, PAdES, XAdES or a JAdES signature format, including supported by an ASiC container format. A digital signature is defined as data appended to, or a cryptographic transformation of data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect it against forgery e.g. by the recipient.
    a. Note: [Law (46) of 2021] defines the terms electronic signature, advanced electronic signature, electronic seals and advanced electronic seal. These signatures and seals are created using digital signature technology. AdES digital signatures defined by ETSI are used as supporting technologies for the creation of advanced electronic signatures and seals as defined in [Law (46) of 2021].

2. AdESig-nonQC: AdES supported by a non-qualified certificate for electronic signatures.

3. AdESeal-nonQC: AdES supported by a non-qualified certificate for electronic seals.
4. AdESig-QC: AdES supported by a qualified certificate for electronic signatures.
5. AdESeal-QC: AdES supported by a qualified certificate for electronic seals.
6. AdES-notLicensed: AdES supported by a certificate that could not match with a licensed trust service.
7. QES: AdES supported by a qualified certificate, with the corresponding private key protected by a QSCD.
8. QESig: QES where the certificate is for electronic signatures.
9. QESeal: QES where the certificate is for electronic seals.

2.3 Definitions and abbreviations regarding the content of a certificate

1. QcCompliance: QcStatement standardized by [EN 319 412-5] that can be present in the qcStatements extension of an X.509 certificate. The presence of this QcStatement claims that the certificate is a qualified certificate. According to [EN 319 412-5], the precise meaning of this statement is enhanced by the QcCC statement:
    a. Absence of QcCC: The certificate is an EU qualified certificate that is issued according to EU laws: Directive 1999/93/EC or the Annex I, III or IV of the Regulation (EU) No 910/2014 whichever is in force at the time of issuance.
    b. Presence of QcCC: The certificate is a qualified certificate that is issued according to the laws of the country determined by the value of the QcCC statement.

    Its formal syntax is id-etsi-qcs-QcCompliance. According to [EN 319 412-5], the precise meaning of this statement is enhanced by the QcType statement:
    a. Presence of QcType: The certificate is issued for electronic signatures or electronic seals as of the type declared by the QcType.
    b. Absence of QcType: The absence of this statement is not allowed when the QcCompliance statement is present.

2. QcType: QcStatement standardized by [EN 319 412-5] that can be present in the qcStatements extension of an X.509 certificate. The presence of this QcStatement claims that a qualified certificate is issued as one specific type when used in combination with the QcCompliance defined above. When used on its own it indicates that it is used for the purposes of electronic signatures, seals or websites for non-qualified certificates. Its formal syntax is id-etsi-qcs-QcType. For the moment, three values are defined but only the first two are used for AE qualified certificates:
    - id-etsi-qct-esign (for the purpose of electronic signatures)
    - id-etsi-qct-eseal (for the purpose of electronic seals)
    - id-etsi-qct-web (for web site authentication)

    Note: This statement, without the one defined in clause 4.2.1 of [EN 319 412-5], can be potentially used in any regulatory environments which use electronic signatures, electronic seals or web site authentication with the same meaning.
3. QcCCLegislation, abbreviated in QcCC: QcStatement standardized by [EN 319 412-5] that can be present in the qcStatements extension of an X.509 certificate. Its formal

syntax is id-etsi-qcs-QcCCLegislation. The precise meaning of the statement is enhancing the QcCompliance:

a. Absence of QcCC: The certificate is an EU qualified certificate that is issued according to EU laws: Directive 1999/93/EC or the Annex I, III or IV of the Regulation (EU) No 910/2014 whichever is in force at the time of issuance.

b. Presence of QcCC: The certificate is a qualified certificate that is issued according to the laws of the country determined by the value of the QcCC statement.

4. QcQSCD: QcStatement standardized by [EN 319 412-5] that can be present in the qcStatements extension of an X.509 certificate. The presence of this Qcstatement claims that the private key related to the certified public key resides in a QSCD according to the Regulation (EU) No 910/2014 or a secure signature creation device (SSCD) as defined in the Directive 1999/93/EC. Its formal syntax is id-etsi-qcs-QcSSCD.

2.4 Definitions and abbreviations regarding the content of a trusted list

More information can be found in version [TS 119 612]. This standard is profiled to the UAE context in the [TDRA TL Resolution].

1. Q/CA/ForeSignatures: Service type identifier as defined in the [TDRA TL Resolution] (http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/CA/ForeSignatures): qualified trust service issuing qualified certificates for electronic signatures.
2. Q/CA/ForeSeals: Service type identifier as defined in the [TDRA TL Resolution] (http://uri.trustservices.gov.ae/TrstSvc/Svctype/Q/CA/ForeSeals): qualified trust service issuing qualified certificates for electronic seals.
3. Q/CA/ForXX: abbreviation for Q/CA/ForeSignatures and Q/CA/ForeSeals
4. nonQ/CA/ForeSignatures: Service type identifier as defined in the [TDRA TL Resolution] (http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/CA/ForeSignatures): non-qualified trust service issuing non-qualified certificates for electronic signatures.
5. nonQ/CA/ForeSeals: Service type identifier as defined in the [TDRA TL Resolution] (http://uri.trustservices.gov.ae/TrstSvc/Svctype/nonQ/CA/ForeSeals): non-qualified trust service issuing non-qualified certificates for electronic seals.
6. nonQ/CA/ForXX: abbreviation for nonQ/CA/ForeSignatures and nonQ/CA/ForeSeals. For the purpose of the present document, this excludes nonQ/CA/ForWebsiteAuthentication.
7. (non)Q/CA/ForXX: abbreviation for Q/CA/ForXX and nonQ/CA/ForXX.
8. SDI: Service Digital Identity unambiguously identifying the trust service. The standard imposes it to contain at least one certificate (if the service uses PKI public-key technology). In the present document, the SDI is said to be “catching” a sigCert if a path can be found from the sigCert up to the SDI.
9. Sie:Q:QcStatement : Service information extension / qualification that is composed of one or more criteria and a qualifier. The qualifier applies to the sigCert only if the sigCert meets the criteria. In the present document, “a Sie:Q:QcStatement is present” shall be understood as “a Sie:Q:QcStatement that applies to the sigCert is present”. The criteria are then said to “catch” this sigCert.
10. Sie:Q:notQualified : Service information extension / qualification that is composed of criteria and a qualifier. The qualifier applies to the sigCert only if the sigCert meets the

criteria. In the present document, “a Sie:Q:notQualified is present” shall be understood as “a Sie:Q:notQualified that applies to the sigCert is present”. The criteria are then said to “catch” this sigCert.

11. Sie:Q:QCForXX: Service information extension / qualification that is composed of criteria and a qualifier. The qualifier applies to the sigCert if and only if the sigCert is qualified and meets the criteria. In the present document, “a Sie:Q:QCForXX is present” shall be understood as “a Sie:Q:QCForXX that applies to the sigCert is present”. The criteria are then said to “catch” this sigCert. QCForXX is an abbreviation for QCForESig / QCForESeal.
12. Sie:Q:QCXXQSCD : Service information extension / qualification that is composed of criteria and a qualifier. The qualifier applies to the sigCert only if the sigCert is qualified and meets the criteria. In the present document, “a Sie:Q:QCXXQSCD is present” shall be understood as “a Sie:Q:QCXXQSCD that applies to the sigCert is present”. The criteria are then said to “catch” this sigCert. QCXXQSCD is an abbreviation for QCWithQSCD / QCNoQSCD.
13. Sie:nonQ:nonQCForXX: Service information extension / non-qualification that is composed of criteria and a non-qualifier. The non-qualifier applies to the sigCert if and only if the sigCert is non-qualified and meets the criteria. In the present document, “a Sie:nonQ:nonQCForXX is present” shall be understood as “a Sie:nonQ:nonQCForXX that applies to the sigCert is present”. The criteria are then said to “catch” this sigCert. nonQCForXX is an abbreviation for nonQCForESig / nonQCForESeal / nonQCForWSA.
14. Sie:nonQ:notNonQualified : Service information extension / non-qualification that is composed of criteria and a non-qualifier. The non-qualifier applies to the sigCert only if the sigCert meets the criteria. In the present document, “a Sie:nonQ:notNonQualified is present” shall be understood as “a Sie:nonQ:notNonQualified that applies to the sigCert is present”. The criteria are then said to “catch” this sigCert.

2.5 Other definitions and abbreviations

1. OG: United Arab Emirates Official Gazette.
2. QSCD: qualified signature creation device, as defined in the Regulation (EU) No 910/2014 (the “eIDAS” Regulation[1]).

3. Underlying principles

The algorithm presented in the next section is based on the following principles:

3.1 (non)Q/CA/ForXX trust service(s) matching the sigCert

1. A Q/CA/ForXX entry in a TL will correspond to the sigCert if and only if:
   a. A path can be found from the sigCert up to the SDI of this entry.
   b. The type of the sigCert is in line with the type of qualified certificates this service is issuing, taking into account possible overruling of the TL (see below the section on

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

overruling). Even if the SDI is matching, a Q/CA/ForXX entry will not be related to a sigCert if the corresponding types (the type “XX” of Q/CA/ForXX and QcType respectively) are not matching.

c. The certificate is confirmed to be qualified, taking into account possible overrule in the TL entry (see below the section on overruling). Even if the SDI is matching, a Q/CA/ForXX entry will not be related to a sigCert if the sigCert is not qualified.

For instance, when looking for the Q/CA/ForXX entry that catches the sigCert:

a. Several Q/CA/ForXX entries with the same catching SDI but with different type “XX” may exist. The entry catching the sigCert will be the one with the appropriate type “XX”.
b. One Q/CA/ForXX entry may exist with a catching SDI. This entry will not be catching the sigCert because the sigCert is not qualified.
c. One Q/CA/ForXX entry may exist together with a nonQ/CA/ForXX, with the same catching SDI and the same type “XX”. If the certificate is not qualified, the Q/CA/ForXX entry will not be considered as catching it (and so will not be considered as applicable).

A nonQ/CA/ForXX entry in a TL will correspond to the sigCert if and only if:

a. A path can be found from the sigCert up to the SDI of this entry.
b. The type of the sigCert is in line with the type of non-qualified certificates this service is issuing, taking into account possible overruling of the TL (see below the section on overruling). Even if the SDI is matching, a nonQ/CA/ForXX entry will not be related to a sigCert if the corresponding types (the type “XX” of nonQ/CA/ForXX and QcType respectively) are not matching.
c. The certificate is confirmed to be non-qualified, taking into account possible overrule in the TL entry (see below the section on overruling). Even if the SDI is matching, a nonQ/CA/ForXX entry will not be related to a sigCert if the sigCert is qualified.

A further check shall be performed to rule out inapplicable cross-certification or root signing (e.g. outside of UAE): When present, the organizationIdentifier attribute of the issuer of the sigCert, or the issuerAltName field, should match the TSP name or the TSP trade name of the TSP service entry.

3.2 Overruling by the TL in Q/CA/ForXX trust services

1. Sie:Q:QcStatement or Sie:Q:notQualified qualifier in the TL overrules the QcCompliance statement present in the sigCert, if any.
   Note: As stated in its definition above, it is also subject to the condition that the corresponding criteria is catching this sigCert.
2. Sie:Q:QCXXQSCD qualifier(s) in the TL overrule(s) the QSCD statement present in the sigCert, if any.
   Note: As stated in its definition above, it is also subject to the conditions that the corresponding criteria is catching this sigCert, and that this sigCert is concluded to be qualified.

3. Sie:Q:QCForXX qualifier in the TL overrules the QcType statement present in the sigCert, if any.
   Note: As stated in its definition above, it is also subject to the conditions that the corresponding criteria is catching this sigCert, and that this sigCert is concluded to be qualified.

3.3 Overruling by the TL in nonQ/CA/ForXX trust services

1. Sie:Q:nonQCForXX qualifier in the TL overrules the QcType statement present in the sigCert, if any.Note: As stated in its definition above, it is also subject to the conditions that the corresponding criteria is catching this sigCert, and that this sigCert is concluded to be non-qualified.

3.4 Two moments in time to be considered when validating a signature or a seal

There are two moments in time to be considered when validating a qualified electronic signature under Article 20 of [Law (46) of 2021]:

- Time of issuance [2]of the certificate;
- Time of signing.

The type of the certificate at the time of issuance and at the time of signing regarding shall be the same. The algorithm will raise an error if the type has changed in between.

The qualified status of the certificate at the time of issuance and at the time of signing regarding shall be the same. The algorithm will raise an error if the type has changed in between.

3.5 Qualified status of a certificate is lost if the qualified status of the issuing trust service entry in the TL is withdrawn

The qualified status of a certificate for electronic signatures is **not immutable** after its issuance. According to Article 1 of [Law (46) of 2021], a certificate for electronic signatures is qualified whether:

1. It meets the requirements laid down in Article 21 of the [Reg (28) 2023] ;
2. And it is issued by a qualified TSP.

Qualified certificates already issued by a qualified TSP lose their qualified status[3] if they fail to continue to comply with Article 1 of [Law (46) of 2021].

[2] In case of a certificate issued before the entry into force of the [Law (46) 2021] and benefitting from a transition measure, the trusted list will contain the relevant information at that moment.

[3] The certificates shall actually get revoked. Because of the licensing scheme, for a trust service losing its qualified status means losing its license. Its activities shall stop, and all previously-issued certificates shall be revoked. Although the case should not happen, the algorithm still makes sure that these certificates shall not be considered as qualified.

A TSP that is not qualified anymore for provision of a qualified trust service for the issuance of QC of a specific type (e.g. for electronic signatures) cannot issue **new QC** for that specific type (e.g. for electronic signatures).

Based on the way in which the TL currently operates in accordance with the relevant standard, setting the status of the trust service entry in the TL as withdrawn has the result that **previously issued QC** for electronic signature no longer can be considered as qualified.

In brief, as explained in the section "Interpretation of the TL content" of the [TDRA TL Resolution], in the TL, the withdrawal of qualified status of the issuing trust service entry shall be interpreted as implying that:

- Newly issued certificates are not qualified[4];
- Already issued qualified certificates are no longer to be considered as qualified.

3.6 Interpretation of QcType in the sigCert

The QcType shall be present in the sigCert, whether the QcCompliance is present or not. Depending on the QcStatements in the TL, the certificate will be either qualified (QC) or non-qualified (nonQC).

Following [EN 319 412-5] Section 4.2.3, the QcType declares that a certificate is issued as one and only one of the purposes of electronic signature, electronic seal or website authentication. Therefore, when following this standard, only one QcType is allowed within a sigCert. However, [TS 119 615] tolerates the case where two or more QcType are present but only if one (applicable) Sie:Q:QCForXX or Sie:nonQ:nonQCForXX is present in the TL to overrule this QcType.

Some specific cases (cf. [TS 119 615] and [EN 319 412-5]) shall be considered such as:

- Absence of QcCompliance, overruled by Sie:Q:QcStatement in the TL, and absence of QcType (in the absence of further overruling in the TL) shall lead to conclude that the overruling in the TL is incomplete as it should contain an indication of type as well (Sie:Q:QCForXX or Sie:nonQ:nonQCForXX). [TS 119 615] conclusion is then indeterminate: INDET_QC_For_eSig / INDET_QC_For_eSeal.
  This slight difference prevents an algorithm from implementing completely separately the conclusion on the QC status (based on QcCompliance and Sie:Q:QcStatement / Sie:Q:NotQualified) and the conclusion on the type (based on QcType and Sie:Q:QCForXX / Sie:nonQ:nonQCForXX).

Lastly, a certificate for WSA is not accepted neither as a certificate for electronic signatures nor as a certificate for electronic seals.

[4] The comment applies here: this situation shall not happen. However, the algorithm makes sure they shall not be considered as qualified.

4. Preliminary steps and checks

There can be problems:

- When accessing and validating the TL.
- When incompatible statements are found in the TL.
- When incompatible statements are found between the content of the sigCert and the TL.

The subsections below describe consistency checks related to these potential problems. If such consistency check fails:

- In most cases, a warning is included in the validation report.
- In some critical cases, a full stop of the process, with the result being an error.

4.1 Access the TL

- General checks on TL
    a. Availability: if not available immediately, ensure a certain freshness.
    b. Not expired (list issue date and time, next update).
    c. Correctly signed (based on the applicable Official Gazette publication and pivot TL(s) “chain”). The applicable pivot TL mechanism is described in that same publication.
- Failures of these checks are reported as warnings in the validation report.

4.2 Identify (non)Q/CA/ForXX entry(ies) in the TL as trust anchor(s), and detect inconsistencies

Identify in the TL the (non)Q/CA/ForXX entry(ies) to which a path can be built from the sigCert. This part is further detailed in the next section.

The following coherence checks on these TL entry(ies) are performed:

1. The following Sie:Q:* statements are mutually exclusive and will raise an error:
    a. QcStatement and NotQualified for the same sigCert under consideration.
    b. QcForeSig, QcForeSeal for the same sigCert under consideration.
2. The following Sie:nonQ:* statements are mutually exclusive and will raise an error:
    a. nonQcForeSig, nonQcForeSeal, (nonQcForWSA) for the same sigCert under consideration.
3. One shall not be able to conclude both QSCD and not QSCD. The following combination are inconsistent:
    b. QcNoQSCD together with QcWithQSCD
4. Q/CA/ForXX and Sie:Q:QcForXX shall be consistent, i.e. if Sie:Q:QcForXX is forcing certificates to be for eSignature / eSeal, then a corresponding “XX” in Q/CA/ForXX shall be declared for that trust service.
5. nonQ/CA/ForXX and Sie:nonQ:nonQcForXX shall be consistent, i.e. if Sie:nonQ:nonQcForXX is forcing certificates to be for eSignature / eSeal, then a corresponding “XX” in nonQ/CA/ForXX shall be declared for that trust service.

6. The organizationIdentifier or the issuerAltName of the sigCert shall match the TSP Name or the TSP trade name. Note: It could be located at other places in the sigCert, but the algorithm only checks these 2.

5. Main algorithm

The algorithm is composed of 3 main parts, based on Article 20 of [Law (46) of 2021]:

a. Determining if the sigCert was a (non)QC for eSig / eSeal (and is valid) at the time of issuance.
b. Determining if the sigCert was a (non)QC for eSig / eSeal and is related to a QSCD (and is valid) at the time of signing.
c. Determining if the signature is an AdES. This step is based on ETSI EN 319 102-1 and will not be developed further in the present document.

Provided that it is parametrized with a date, the first 2 parts can be factorized into:

a. Determining the qualified status of the sigCert, and its type.
b. At the time of signing: If the sigCert is qualified, determining if the corresponding private key is protected by a QSCD.

For executing these steps, one has to find which (non)Q/CA/ForXX entry(ies) is(are) corresponding to the sigCert. Because of the overruling of the trusted list on the sigCert content, several (non)Q/CA/ForXX entries may catch the sigCert at first, and so the algorithm considers all these (non)Q/CA/ForXX entry(ies) catching the sigCert, irrespective of the service status, and irrespective of the “XX” type in the (non)Q/CA/ForXX. For instance:

a. A Q/CA/ForeSignatures might catch a qualified sigCert with QcType eSeal if there is an overruling Sie:Q:QcForeSig catching this sigCert and forcing it to be for electronic signatures.
b. A Q/CA/ForXX might catch a non-qualified sigCert if there is an overruling Sie:Q:QcStatement catching this sigCert and forcing it to be qualified.

For each applicable entry, conclusion based on the 3 subsections below can be: QESig / QESeal / AdESig-QC / AdESeal-QC / AdESig-nonQC / AdESeal-nonQC / AdES-not licensed / Indeterminate cases from [TS 119 615].

However, after considering all these (non)Q/CA/ForXX entries corresponding to the sigCert, applying for each the rules presented in the following subsections, there should remain only one applicable (non)Q/CA/ForXX entry and one conclusion:

a. If there is no applicable (non)Q/CA/ForXX entry left, the sigCert is considered as issued by a non-licensed trust service.
b. If there is more than one applicable (non)Q/CA/ForXX entry left, and their conclusions are different, it raises an error and the algorithm stops.
c. If there is more than one applicable (non)Q/CA/ForXX entry left, and their conclusions are coherent, the algorithm shall issue a warning and result in this common conclusion.

d. If there is more than one applicable (non)Q/CA/ForXX entry left, and their conclusions are identical, it raises a warning and the algorithm conclusion is this one.

5.1 (Non) Qualified status of the sigCert

a. If the Q/CA/ForXX entry under consideration is not in granted status, the sigCert is not qualified.
b. If the nonQ/CA/ForXX entry under consideration is not in granted status, the sigCert is not non-qualified.
c. If the Q/CA/ForXX entry under consideration is overruling the qualified status of the sigCert (Sie:Q:QcStatement or Sie:Q:NotQualified), then the conclusion on the sigCert qualification is based on the Q/CA/ForXX entry, whatever is present in the sigCert.
d. If the Q/CA/ForXX entry under consideration is not overruling the qualified status of the sigCert, then the conclusion on the sigCert qualification is based on the sigCert content:

- The algorithm considers the presence of QcCompliance and QcCC = “AE”

5.2 Type of the sigCert

- If the last subsection concluded on the sigCert being not licensed, then the type of the sigCert is as declared by the QcType.
- If the last subsection concluded on the sigCert being (non-)qualified, this conclusion is only applicable provided that the type of certificate does match. The type declared in the certificate and the type declared in the Q/CA/ForXX entry under consideration do match if:

    a. There is an overruling Sie:(non)Q:(non)QcForXX catching the sigCert. The conclusion on the type is then XX, whatever is present in the sigCert.
    b. There is no overruling Sie:(non)Q:(non)QcForXX catching the sigCert, and the QcType of the sigCert is the same as the “XX” type of (non)Q/CA/ForXX. The conclusion is then QcType.

    If these two types do not match, then the (non)Q/CA/ForXX entry is not applicable, and the algorithm removes it from the list of potential (non)Q/CA/ForXX entries.

5.3 QSCD status

If sigCert is not qualified, no conclusion is drawn on QSCD. The algorithm proceeds to this step only if in the last subsection the sigCert was concluded to be qualified. Then:

a. If there is an overruling Sie:Q:QCXXQSCD catching the sigCert, conclusion on QSCD is drawn from Sie:Q:QCXXQSCD, whatever is present in the sigCert.
b. If no overruling Sie:Q:QCXXQSCD is catching the sigCert , conclusion on QSCD is drawn based on the sigCert content:

- The algorithm considers the presence of QcQSCD.