Requirements for qualified signature verification according to eIDAS

Version: 1.0

2025-04-04

Contents

1 Introduction

This paper examines the issues of the verification of qualified electronic signatures under the eIDAS Regulation from a legal perspective.

The purpose of this document is to set out the rules that generally apply to the verification of qualified signatures.

This is necessary because:

- There is no mandatory standard to be used in the framework of eIDAS1
- There is no mandatory standard expected to be used under eIDAS2 because, according to Article 32(1)(2), compliance with the standard is presumed to be compliance with the legislation.

Therefore, it is necessary to introduce the concept of **"Article 32 signature verification"** in any case, because it is the one that is binding for everyone.

By analyzing the relevant points of the legislation, it is possible to determine/derive the acceptance requirements for the content of the certificates, the timing of the revocation information, the verification of each signature level.

The following 2. Summary chapter summarizes the interpreted requirements, with detailed derivations in each clarifying subchapter.

2 Summary

The verification of a qualified electronic signature should check the fulfilment of the requirements in the following subsections.

2.1 Requirements concerning the content of the certificate

The signatory certificate must contain the following information:

- Subject data:
    - *commonName* (CN) – name of the Subject,
    - *givenName* (GN) – given name of the Subject,
    - *surname* (SN) – surname of the Subject,
    - *Subject:serialNumber* – the serial number ensuring the uniqueness of the Subject.

  Note: ETSI EN 319412-2 chapter 4.2.4 requires the country (C) to be indicated, although it is not mandatory from eIDAS.

- Issuer data:
    - *commonName* (CN) – Issuer's name,
    - *organization* (O) – name of the registered entity of the Trust Service Provider (TSP),
    - *organizationIdentifier* – the identification code of the TSP in the register,
    - *countryName* (C) – the country of registration of the TSP.
- Certificate extensions:
    - *authorityInfoAcces:OCSP* and/or *cRLDistributionPoints*
      or, in their absence, the *noRevAvail* extension - where to find the revocation information (CRL, OCSP) or information about the revocation information
    - *qcStatements* extensions:
        - *QcCompliance* – the indication of the qualified status,
        - *QcType* with *esign* value – the indication of the qualified signatory certificate,
        - *QcSSCD* – if the private key for the certificate is generated on a QSCD device, it shall be included.
    - *authorityInfoAcces:CAIssuers* – the download address of the signing CA certificate that signed the signer certificate.
- Other certificate data
    - the public key of the Subject
    - the signature of the CA on the certificate
    - the validity of the certificate

2.2 Requirements for signature levels

The verification requirements for each signature level are summarized in the table below.

Level	Level includes…	Explanation	Is it suitable for long-term preservation?	Is additional information needed for the verification	The limit to how long the validity of a signature can be established
B	signature only	As there is no timestamp or revocation information in the signature at this level, the validity of the signature cannot be established by default.	No.	Yes, a CRL or OCSP response is required.	**On their own:** Not ascertainable. **Additional information provided:** Within the validity period of the signing certificate (and its chain).
T	signature with time stamp	Since the time stamp at this level provides authentic information about the date of signature, the validity of the signature can be established within the validity period of the time stamp certificate (and its chain).	No.	Yes, a CRL or OCSP response is required.	**On their own:** Not ascertainable. **Additional information provided:** Within the validity period of the time stamp certificate (and its chain). (A timestamp certificate is typically valid much longer than a signer certificate.)

Level	Level includes…	Explanation	Is it suitable for long-term preservation?	Is additional information needed for the verification	The limit to how long the validity of a signature can be established
LT	signature with time stamp and subsequent revocation information attached	Since the attached revocation information is not protected by a time stamp (i.e. it is attached as quasi B level signed information), its maximum acceptance time should be set on the basis of the B signature level.	No.	No. If the CRL or OCSP response has expired, a new CRL or OCSP response must be obtained.	**On their own:** Within the validity period of the revocation information (and its chain). **With additional information supplied:** Within the validity period of the time stamp certificate (and its chain) and the revocation information (and its chain).
LTA	signature with time stamp and revocation information, followed by archival time stamp	An archival timestamp protects all the contents underneath it, so that their validity can be established as long as the verification is carried out within the validity period of the outermost archival timestamp (and its chain).	Yes.	No.	Within the validity period of the archival time stamp certificate (and its chain).

2.3 Trusted list requirements

- The issuer of a qualified certificate on the trusted list must have a "granted" status at the time the signing certificate is issued and at the time it is signed.
- The revocation status of a chain element on the trusted list no longer needs to be checked.

2.4 Requirements for revocation information

- The revocation information (CRL or OCSP response) must be issued after the date of signature (grace period), i.e. both the CRL and the OCSP response are signed/issued by the trust service provider after the date of signature (the value of *thisUpdate* of the CRL, OCSP response is later than the date of signature.)
- The revocation information, if it does not contain an ArchiveCutoff (OCSP) or ExpiredCertsOnCRL (CRL) extension, can only be accepted within the validity period of the certificate.

2.5 Requirement to display certificatePolicies:userNotice:Explicit text field

- If the certificate does not contain a *certificatePolicies:userNotice:Explicit text* field, the certificate has no explicit restrictions, and signature verification can proceed.
- If it is not empty, its content must be displayed to the verifier during the verification process to allow the verifier to assess the restrictions and decide whether to accept the signature.

3 Detailed explanation

The following subsections analyze the legal requirements of Article 32, and Article 26 and Annex I referred to therein.

In the section on Article 32, the contents of the chapters referred to are summarized where appropriate and explained in detail in their respective chapters.

3.1 eIDAS Article 32.

The eIDAS Regulation provides the rules for the validation of qualified signatures in Article 32(1), and a signature verified in accordance with this Article is considered a valid signature. The following subsections explain the specific requirements.

3.1.1 (a) the signatory's certificate meets the requirements of Annex I

The legal requirement

(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;

Implementation of the requirement

In short, this requirement means that a qualified signatory certificate must contain the following elements:

- Subject data:
  - *commonName* (CN) – name of the Subject,
  - *givenName* (GN) – given name of the Subject,
  - *surname* (SN) – surname of the Subject,
  - *Subject:serialNumber* – the serial number ensuring the uniqueness of the Subject.

  Note: ETSI EN 319412-2 chapter 4.2.4 requires the country (C) to be indicated, although it is not mandatory from eIDAS.

- Issuer data:
  - *commonName* (CN) – Issuer's name,
  - *organization* (O) – name of the registered entity of the Trust Service Provider (TSP),
  - *organizationIdentifier* – the identification code of the TSP in the register,
  - *countryName* (C) – the country of registration of the TSP.
- Certificate extensions:
  - *authorityInfoAcces:OCSP* and/or *cRLDistributionPoints* or, in their absence, the *noRevAvail* extension - where to find the revocation information (CRL, OCSP) or information about the revocation information
  - *qcStatements* extensions:
    - *QcCompliance* – the indication of the qualified status,
    - *QcType* with *esign* value – the indication of the qualified signatory certificate,
    - *QcSSCD* – if the private key for the certificate is generated on a QSCD device, it shall be included.
  - *authorityInfoAcces:CAIssuers* – the download address of the signing CA certificate that signed the signer certificate.
- Other certificate data
  - the public key of the Subject
  - the signature of the CA on the certificate
  - the validity of the certificate

A detailed are in chapter **3.3 eIDAS Annex I. – the content of the** qualified signing certificate .

3.1.2 (b) the certificate was issued by a qualified trust service provider and was valid at the time of signature

The legal requirement

(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

These are in fact two main sub-requirements, which can be broken down into further sub-requirements:

i. verification of the qualified certification authority on the EU trusted list,

ii. verification that the certificate was valid at the time of signing, i.e.:

   a. the signature took place within the validity period of the signing certificate (notBefore, notAfter),

   b. the signing certificate was not revoked at the time of signature.

   c. checking revocation information to see if it can contain status information for the certificate being checked.

Implementation of the requirement

We can check each sub-requirement separately.

i. The verification of the qualified certificate issuer on the EU Trusted List should be done by verifying that the issuing trust service provider's certificate was on the Trusted List with a "granted" entry at the time of issuing the signing certificate and that it is not in a "withdrawn" state at the time of signing.
The TSP certificates shall be checked automatically against EUTL. You can check the validity manually on this page: https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls

ii. Verifying the signer certificate validity at the signing time:

   a. the time of signature must fall between the notBefore and notAfter boundaries of the signing certificate

   b. an **OCSP or CRL response issued after the date of signature** indicates that the certificate is not revoked.
   The CRL or OCSP response after the signature date is required because the pre-signature CRL or OCSP response cannot yet contain revocation/suspension information, only the revocation information issued after the signature can provide that information. Therefore, **a CRL or OCSP response issued after the signature date is required.** (The maximum value of RevocationFreshnessConstraints according to ETSI TS 119 172-4 is therefore 0.)

   The certificate is **not revoked** if the serial number is **not on the CRL** and the **OCSP** response shows a **"good"** status.

   Note: Adobe Reader, in particular for embedded revocation information, checks whether the signature is within the validity period of the CRL or OCSP response. This is incorrect because, for the reasons just described, the revoked status of a given certificate may not yet be reflected in the CRL or OCSP response issued prior to signing. This is why it is possible that the validity of a signature may be shown by Adobe Reader as valid even if the signing certificate was revoked before signing.

c. verify that the revocation information of the signing certificate was issued within the validity period of the certificate or contains the *ArchiveCutoff* (OCSP) or *ExpiredCertsOnCRL* (CRL) extension. This is necessary because according to RFC 5280, the information shall be available in the certificate’s validity period, if not inserted.

Note: According to eIDAS Article 24 (4), this information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient, so for qualified certificates the use of ArchiveCutoff and ExpiredCertsOnCRL extensions in revocation information is mandatory.

To check the validity of the signature, the validity of the other certificates in the certificate chain must also be checked, and the above method must be applied recursively.

Verification of requirements online, in certificates, and in CRL and OCSP responses

i. Trusted List Verification - It is recommended to automatically check the provider certificates against EUTL. You can check the validity manually at this page: https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls

ii. Checking the validity of the signing certificate:

a. The date of signature must fall within the validity period of the signing certificate:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
        02:36:c1:75:df:72:ff:d3:56:a0:fd:e7:c0:0a
     Signature Algorithm: ecdsa-with-SHA256
     Issuer: C = HU, L = Budapest, O = Microsec Ltd.,
organizationIdentifier = VATHU-23584497, CN = e-Szigno Qualified
CA 2017
        Validity
          Not Before: Mar 29 13:06:27 2023 GMT
          Not After : Mar 28 13:06:27 2026 GMT
```

b. Validation of revocation data:

Checking this in the case of CRL:

The date/time of issue of the revocation information (*LastUpdate*) must be later than the date of signature and must not contain the serial number of the certificate to be checked.

```
Certificate Revocation List (CRL):
    Version 2 (0x1)
    Signature Algorithm: ecdsa-with-SHA256
    Issuer: C = HU, L = Budapest, O = Microsec Ltd.,
organizationIdentifier = VATHU-23584497,
CN = e-Szigno Qualified QCP CA 2017
    Last Update: Feb 11 11:03:03 2025 GMT
    Next Update: Feb 12 12:03:03 2025 GMT
```

Checking this in the case of OCSP:

The date/time of issue of the revocation information (*ThisUpdate*) must be later than the date of signature and the status of the certificate in the OCSP response shall be "good".

```
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = HU, L = Budapest, O = Microsec Ltd.,
organizationIdentifier = VATHU-23584497, CN = e-Szigno Qualified
CA 2017 OCSP Responder
    Produced At: Mar 31 13:00:14 2025 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 24E8D11B26DC92DCA22DFBA2E34708CC3BAA88AA
      Issuer Key Hash: C613FB3C9DB4B6AE2FC6DE7F954FF31EA9D3C6F9
      Serial Number: 0236C175DF72FFD356A0FDE7C00A
    Cert Status: good
    This Update: Mar 31 13:00:14 2025 GMT
        Response Single Extensions:
            OCSP Archive Cutoff:
                Sep 17 21:00:00 2017 GMT
```

c. Check the *ExpiredCertsOnCRL* (CRL) or *ArchiveCutoff* (OCSP) extension in the revocation information

CRL:

By default, openssl does not recognize the ExpiredCertsOnCRL CRL extension, so it displays it as an OID. In the openssl output, the OID 2.5.29.60 should be looked for. The date associated with the ExpiredCertsOnCRL extension must be the date before the date of signature.

(This would typically be the date the CA was issued.)

```
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: ecdsa-with-SHA256
  Issuer: C = HU, L = Budapest, O = Microsec Ltd.,
organizationIdentifier = VATHU-23584497, CN = e-Szigno Qualified
QCP CA 2017
  Last Update: Feb 11 11:03:03 2025 GMT
  Next Update: Feb 12 12:03:03 2025 GMT
  CRL extensions:
      X509v3 Authority Key Identifier:
      07:F6:2C:C2:03:43:5F:76:67:17:B7:A4:81:87:9A:CC:45:30:7D:DE
      2.5.29.60:
      ..20170917210000Z
      X509v3 CRL Number:
          14825
Revoked Certificates:
  Serial Number: 0123456789ABCDEF0123456789
    Revocation Date: May 1 21:00:00 2024 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          Key Compromise
```

For OCSP:

Openssl knows the *ArchiveCutoff* OCSP response so it can be interpreted from the OCSP response.

In the openssl output, the *OCSP Archive Cutoff* extension should be looked up. The date associated with the *OCSP Archive Cutoff* extension must be a date prior to the date of the signature.

(This would typically be the date the CA was issued.)

```
        OCSP Response Data:
            OCSP Response Status: successful (0x0)
            Response Type: Basic OCSP Response
            Version: 1 (0x0)
            Responder Id: C = HU, L = Budapest, O = Microsec Ltd.,
        organizationIdentifier = VATHU-23584497, CN = e-Szigno Qualified CA 2017
        OCSP Responder
            Produced At: Mar 31 13:00:14 2025 GMT
            Responses:
Certificate ID:
              Hash Algorithm: sha1
              Issuer Name Hash: 24E8D11B26DC92DCA22DFBA2E34708CC3BAA88AA
              Issuer Key Hash: C613FB3C9DB4B6AE2FC6DE7F954FF31EA9D3C6F9
              Serial Number: 0236C175DF72FFD356A0FDE7C00A
            Cert Status: good
            This Update: Mar 31 13:00:14 2025 GMT
                Response Single Extensions:
                    OCSP Archive Cutoff:
                        Sep 17 21:00:00 2017 GMT
```

3.1.2.1 The validity of each signature level

Since the requirement is to verify the validity of the signature, the conditions under which each signature level can be successfully verified must be addressed, as summarized in the following table. In cases outside these limits, the validity of a signature under Article 32 cannot be established.

Level	Level includes…	Explanation	Is it suitable for long-term preservation?	Is additional information needed for the verification	The limit to how long the validity of a signature can be established
B	signature only	As there is no timestamp or revocation information in the signature at this level, the validity of the signature cannot be established by default.	No.	Yes, a CRL or OCSP response is required.	**On their own:** Not ascertainable. **Additional information provided:** Within the validity period of the signing certificate (and its chain).
T	signature with time stamp	Since the time stamp at this level provides authentic information about the date of signature, the validity of the signature can be established within the validity period of the time stamp certificate (and its chain).	No.	Yes, a CRL or OCSP response is required.	**On their own:** Not ascertainable. **Additional information provided:** Within the validity period of the time stamp certificate (and its chain). (A timestamp certificate is typically valid much longer than a signer certificate.)

Level	Level includes…	Explanation	Is it suitable for long-term preservation?	Is additional information needed for the verification	The limit to how long the validity of a signature can be established
LT	signature with time stamp and subsequent revocation information attached	Since the attached revocation information is not protected by a time stamp (i.e. it is attached as quasi B level signed information), its maximum acceptance time should be set on the basis of the B signature level.	No.	No. If the CRL or OCSP response has expired, a new CRL or OCSP response must be obtained.	**On their own:** Within the validity period of the revocation information (and its chain). **With additional information supplied:** Within the validity period of the time stamp certificate (and its chain) and the revocation information (and its chain).
LTA	signature with time stamp and revocation information, followed by archival time stamp	An archival timestamp protects all the contents underneath it, so that their validity can be established as long as the verification is carried out within the validity period of the outermost archival timestamp (and its chain).	Yes.	No.	Within the validity period of the archival time stamp certificate (and its chain).

3.1.3 (c) was signed by the person who was expected to sign, and signed as expected

The legal requirement

(c) the signature validation data corresponds to the data provided to the relying party;

Examination of the requirement

The person in the signing certificate should be compared by the verifier with the person from whom he expects the signature.
Furthermore, **as part of this requirement, it is also necessary to check that the signing certificate for the signature does not contain any usage restrictions** that would prevent the certificate from being accepted.

3.1.3.1 Examination of the certificate's restrictions of use

The legal requirement

2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

Examination of the requirement

According to eIDAS Article 13 (2), if the trust service is subject to restrictions, the liability of the trust service provider in relation to the restrictions can only be excluded if these restrictions are known to third parties, and therefore these restrictions are placed in the certificate.

Such restrictions may include:

- Restrictions on the use of the Certificate
- Restrictions on the use of keys

3.1.3.1.1 Use restriction of the Certificate

Examination of the requirement

Specific restrictions on the use of the certificate are typically textual restrictions, with space for them in the *certificatePolicies:userNotice:Explicit text* field.

If this field is present in the certificate, it shall be presented to the user during the verification process, according to RFC 5280 Chapter 4.2.1.4, and indicate that the signature is only acceptable if the above field does not contain any restriction on acceptability.

Article 13(3) provides Member States with additional regulatory options on this issue.

In the case of Hungary, this contains a prohibitive provision, according to § 101 (2) of the DCA. (Digital Citizenship Act): the signatory is also obliged to comply with the restrictions and cannot abuse them.

3.1.3.1.2 Use restriction of the keys

Examination of the requirement

The *PrivateKeyUsagePeriod* extension can be used to restrict the use of the key. This is not used for signing certificates but can be used for timestamp certificates.

If this extension is included in a certificate, signing with the associated key shall be only accepted if the signing time is within the time period included in the *PrivateKeyUsagePeriod* extension. For timestamps, this means that the timestamp is valid if it was created within this time period.

Examination of the requirement in the certificate

In the openssl output, look for the Private Key Usage Period. The date of signature must fall within the time period indicated in this extension.

```
X509v3 Private Key Usage Period:
   Not Before: Jan 2 16:15:01 2025 GMT, Not After: Mar 31 15:15:00 2026 GMT
```

3.1.4 (d) the verifier receives the certificate and that uniquely identifies the signatory

The legal requirement

(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

Examination of the requirement

A signature certificate embedded in a signature container (format) fulfils this requirement, so using PADES, XADES, CADES, ASIC signature formats this requirement is certainly met.

For uniqueness, see also ***3.2.3 Subject:serialNumber, the implicit requirement of Article 26(1)(a) and (b)*** *chapter.*

3.1.5 (e) the pseudonymous certificate is clearly marked

The legal requirement

(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

Examination of the requirement

In a pseudonymous certificate, the pseudonym must be entered in the pseudonym field, which uniquely identifies it to the verifier.

If the Subject section of the certificate does not contain a pseudonym field, it is not a pseudonymous certificate.

3.1.6 (f) the signature was created using a QSCD device

The legal requirement

(f) the electronic signature was created by a qualified electronic signature creation device;

Examination of the requirement

If the signing certificate contains the *QcSSCD* QCStatement in the *qcStatements* extension, it is compliant.

For detailed steps on how to check this, see **3.3.10 (j) if the keys are generated on a QSCD** device, its indication section.

3.1.7 (f) the signature is not damaged (cryptographically validable)

The legal requirement

(g) the integrity of the signed data has not been compromised;

Examination of the requirement

If the cryptographic validation of the signature is successful and the signature algorithm is usable, the condition is met.

3.1.8 (h) the signature meets the requirements of Article 26 (advanced signature)

The legal requirement

(h) the requirements provided for in Article 26 were met at the time of signing.

Examination of the requirement

To check this requirement, you only need to check the signature format:

If the signature is in *PADES, XADES, CADES, ASIC* container format and at level *B, T, LT* (and consequently *LTA*), then the signature complies with the requirements of Article 26 on the basis of Commission Implementing Decision 2015/1506 (still in force) under Article 27(4) (now repealed).

Nevertheless, we will go through the requirements of Article 26 in detail in the next chapter.

3.2 eIDAS Article 26.

Article 26 contains the criteria for the validity of an advanced signature.

3.2.1 (a) it is uniquely linked to the signatory

The legal requirement

(a) it is uniquely linked to the signatory;

Examination of the requirement

The content of the signer certificate, if it contains at least the signer's name and *Subject:serialNumber*, clearly associates the signer with his signature, because no other subject can have a certificate with the same content.

Examination of the requirement in certificate

See **3.2.3 Subject:serialNumber, the implicit requirement of Article 26(1)(a) and (b)** chapter.

3.2.2 (b) suitable for identifying the signatory

The legal requirement

(b) it is capable of identifying the signatory;

Examination of the requirement

The content of the signer certificate, if it contains at least the signer's name and *Subject:serialNumber*, is suitable for identifying the signer.

Examination of the requirement in certificate

See **3.2.3 Subject:serialNumber, the implicit requirement of Article 26(1)(a) and (b)** chapter.

3.2.3 Subject:serialNumber, the implicit requirement of Article 26(1)(a) and (b)

Since only the name is required in the signing certificate under Annex I, but it is not sufficient for unambiguous identification, since it is not required for personal names to be unique, Article 26 (1) (a) and (b) requires that qualified signing certificates be provided with an identifier that ensures the unique identification of the subject.

This is the *Subject:serialNumber* field as defined in ETSI EN 319412-2 chapter 4.2.4.

Examination of the requirement in certificate

Using openssl, look for the *serialNumber* field in the *Subject* section of the certificate.

```
Subject: C = HU, L = Budapest, O = Microsec zrt., CN = Teszt Elek, GN = Elek,
SN = Teszt, emailAddress = teszt.elek@microsec.hu, serialNumber =
1.3.6.1.4.1.21528.2.2.3.123
```

3.2.4 (c) the signatory data is most likely to be used only by the signatory

The legal requirement

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control;

Examination of the requirement

Since in the case of a QSCD, the key is located on the QSCD device and the information needed to activate it can only be held by the user, the requirement is met when using a QSCD.

3.2.5 (d) changes to the signed data can be tracked

The legal requirement

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Examination of the requirement

If the cryptographic validation of the signature is successful and the signature algorithm is usable, the condition is met.

3.3 eIDAS Annex I. – the content of the qualified signing certificate

Annex I sets out the requirements for the content of the qualified certificates in points (a) to (j).

We will go through these below, describing the requirement, its interpretation and examples of how to check it.

For verification, openssl outputs are shown in the examples where interpreted.

3.3.1 (a) indication of the type qualified signing certificate in automated form

The legal requirement

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;

Implementation of the requirement

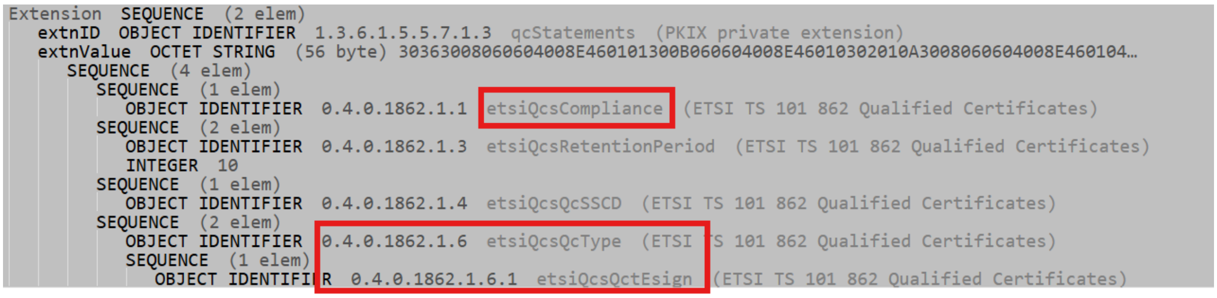
The certificate shall include the following qcStatements extensions according to ETSI EN 319412-5:

- *QcCompliance*
- Its meaning is that the signatory certifies that the certificate was issued in accordance with Annex I (II for stamp; IV for QWAC)
- *QcType*
- This indicates the type of certificate, which must have the value **esign** for a qualified signature *(eseal for a stamp).*

Examination of the requirement in the certificate

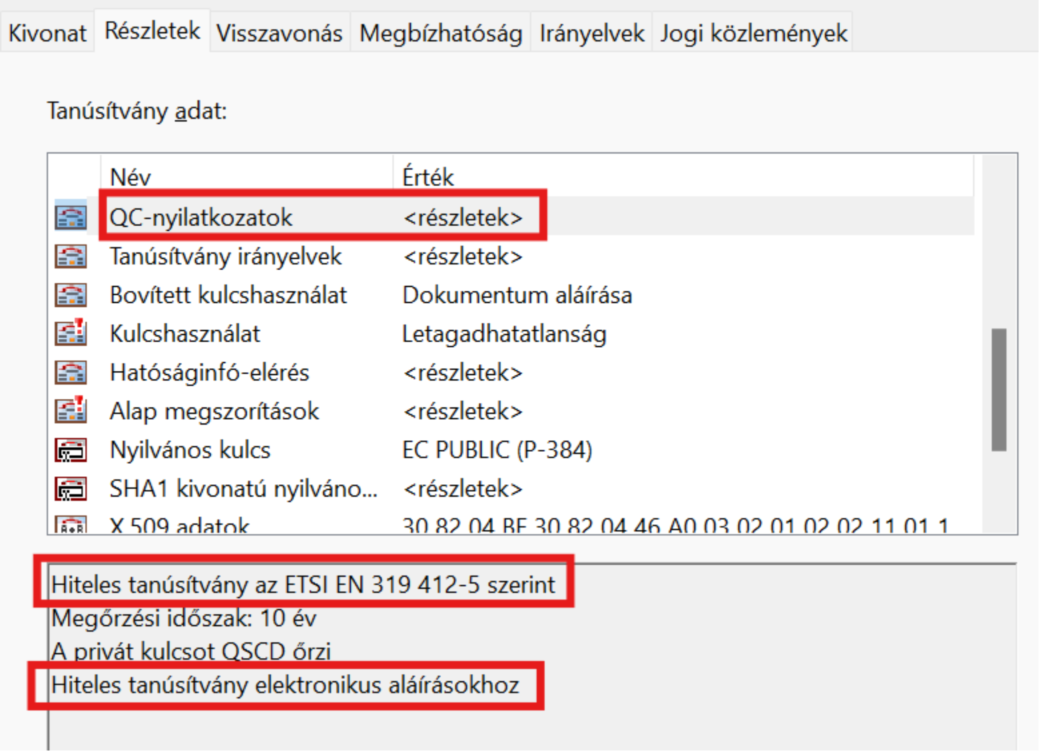
By default, *openssl* does not recognize *qcStatements* extensions, so you can use ASN.1 parser to check.

The ASN.1 structure below shows the *QcCompliance* and *QcType esign* value.



```
Extension  SEQUENCE  (2 elem)
  extnID  OBJECT IDENTIFIER  1.3.6.1.5.5.7.1.3  qcStatements  (PKIX private extension)
  extnValue  OCTET STRING  (56 byte) 3036300806060400 8E460101300B060604008E46010302010A300806060400 8E460104…
    SEQUENCE  (4 elem)
      SEQUENCE  (1 elem)
        OBJECT IDENTIFIER  0.4.0.1862.1.1  etsiQcsCompliance  (ETSI TS 101 862 Qualified Certificates)
      SEQUENCE  (2 elem)
        OBJECT IDENTIFIER  0.4.0.1862.1.3  etsiQcsRetentionPeriod  (ETSI TS 101 862 Qualified Certificates)
        INTEGER  10
      SEQUENCE  (1 elem)
        OBJECT IDENTIFIER  0.4.0.1862.1.4  etsiQcsQcSSCD  (ETSI TS 101 862 Qualified Certificates)
      SEQUENCE  (2 elem)
        OBJECT IDENTIFIER  0.4.0.1862.1.6  etsiQcsQcType  (ETSI TS 101 862 Qualified Certificates)
        SEQUENCE  (1 elem)
          OBJECT IDENTIFIER  0.4.0.1862.1.6.1  etsiQcsQctEsign  (ETSI TS 101 862 Qualified Certificates)
```

Alternatively, you can view QC statements in Adobe Reader under Certificate details.



Tanúsítvány adat:

Név	Érték
QC-nyilatkozatok	<részletek>
Tanúsítvány irányelvek	<részletek>
Bovített kulcshasználat	Dokumentum aláírása
Kulcshasználat	Letagadhatatlanság
Hatóságinfó-elérés	<részletek>
Alap megszorítások	<részletek>
Nyilvános kulcs	EC PUBLIC (P-384)
SHA1 kivonatú nyilváno...	<részletek>
X.509 adatok	30 82 04 BE 30 82 04 46 A0 03 02 01 02 02 11 01 1

Hiteles tanúsítvány az ETSI EN 319 412-5 szerint
Megőrzési időszak: 10 év
A privát kulcsot QSCD őrzi
Hiteles tanúsítvány elektronikus aláírásokhoz

3.3.2 (b) data identifying the qualified service provider

The legal requirement

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:

— for a legal person: the name and, where applicable, registration number as stated in the official records,

Implementation of the requirement

The *Issuer* field in the certificate must contain the minimum information identifying the service provider. These are according to ETSI EN 319 412-2:

- *Organization* – the registered name of the provider organization,
- *OrganizationIdentifier* – the registered identifier of the service provider,
- *commonName* – the name of the provider that refers to itself.

Examination of the requirement in the certificate

Using *openssl*, look for the *C, O, organizationIdentifier* and *CN* fields in the *Issuer* field of the certificate listing.

```
Issuer: C = HU, L = Budapest, O = Microsec Ltd.,
organizationIdentifier = VATHU-23584497,
CN = e-Szigno Qualified CA 2017
```

3.3.3 (c) data identifying the Subject

The legal requirement

(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

Implementation of the requirement

The Subject field in the certificate must contain information that identifies the person.

- *commonName* – name of the Subject,
- *givenName* – given name of the Subject,
- *surname* – surname of the Subject,
- *Subject:serialNumber* – a unique identification number that allows the individual to be uniquely identified, as the subject's name is not sufficient for unique identification due to name mixing. The identifier can be either an identifier generated by a service provider or a unique ID number.

Note: ETSI EN 319412-2 chapter 4.2.4 requires the country (C) to be indicated, although it is not mandatory from eIDAS.

In the case of a pseudonymous certificate (which practically no one requires), the pseudonym should be placed in the *Subject*:*pseudonym* field, which clearly indicates the pseudonymity of the certificate.

Examination of the requirement in the certificate

With *openssl*, look for the *CN, GN, SN*, and *serialNumber* fields in the *Subject* field of the certificate listing.

```
Subject: C = HU, L = Budapest, O = Microsec zrt., CN = Teszt Elek, GN = Elek,
SN = Teszt, emailAddress = teszt.elek@microsec.hu, serialNumber =
1.3.6.1.4.1.21528.2.2.3.123
```

3.3.4 (d) data that can be used to validate a qualified signature

The legal requirement

(d) electronic signature validation data that corresponds to the electronic signature creation data;

Implementation of the requirement

This requirement makes the public key a mandatory part of the certificate.

This means that the certificate must include the *SubjectPublicKeyInfo* section as defined in *RFC 5280.*

Examination of the requirement in the certificate

Using *openssl* to list the certificate, locate the *SubjectPublicKeyInfo* section.

This is different for RSA and ECC keys, the sample below shows a NIST P-256 curve ECC public key.

```
Subject Public Key Info:
    Public Key Algorithm: id-ecPublicKey
    Public-Key: (256 bit)
        pub:
            04:fa:c8:ad:84:e9:4c:e7:28:35:13:d3:c1:89:c2:
            03:90:ef:bb:32:44:12:c0:ee:7a:58:6a:5c:03:13:
            b7:48:eb:12:96:2c:92:58:81:cb:12:4f:ac:d9:ef:
            e6:d9:39:e3:02:47:0f:71:9b:79:ab:58:b0:9b:5b:
            5e:ef:7c:9d:43
         ASN1 OID: prime256v1
         NIST CURVE: P-256
```

3.3.5 (e) the validity period of the certificate

The legal requirement

(e) details of the beginning and end of the certificate's period of validity;

Implementation of the requirement

This requirement makes the validity period of the certificate a mandatory part of the certificate.

This means that the certificate must contain the *notBefore* and *notAfter* values according to *RFC 5280*.

Examination of the requirement in the certificate

Using *openssl*, list the certificate and look for the *notBefore* and *notAfter* values.

```
Validity
    Not Before: Mar 29 13:06:27 2023 GMT
    Not After : Mar 28 13:06:27 2026 GMT
```

3.3.6 (f) the certificate serial number

The legal requirement

(f) the certificate identity code, which must be unique for the qualified trust service provider;

Implementation of the requirement

The first half of the requirement is implemented in the *Certificate:serialNumber* field of the certificate. To fulfil the second half of the requirement to be unique to the service provider, ETSI EN 319411-1 GEN-6.3.3-02A requirement to include a random number in the certificate serial number shall be met.

Examination of the requirement in the certificate

Using *openssl* to list the certificate, look for the Serial Number entry under Certificate.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            02:36:c1:75:df:72:ff:d3:56:a0:fd:e7:c0:0a
```

3.3.7 (g) signature of the Trust Service Provider

The legal requirement

(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

Implementation of the requirement

This requirement makes the signature of the service provider a mandatory part of the certificate.

This means that the certificate must contain the *Signature Algorithm* and *Signature Value* values according to RFC 5280.

Examination of the requirement in the certificate

Using *openssl*, list the certificate and look for the *Signature Algorithm* and *Signature Value* values.

```
Signature Algorithm: ecdsa-with-SHA256
Signature Value:
    30:44:02:20:5e:09:1d:e1:79:92:22:96:36:c3:ef:cd:ef:dc:
    b7:01:97:78:64:4c:08:9d:f4:00:e4:ed:70:8b:dc:d4:cd:5b:
    02:20:54:25:c8:0d:99:89:0d:d6:f7:16:ca:df:46:6e:43:8a:
    d4:ec:d5:f8:90:83:3b:ad:48:67:32:5c:0a:f6:a4:78
```

3.3.8 (h) the download URL of the issuer certificate

The legal requirement

(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;

Implementation of the requirement

This requirement makes it mandatory for the certificate to include a URL where the certificate issuing the certificate can be downloaded.

This means that the certificate must contain the RFC 5280 *authorityInfoAccess* extension with the *CAIssuers* method and a URL as a value where the certificate can be downloaded.

Examination of the requirement in the certificate

Using *openssl* to list the certificate, look for the values *authorityInfoAcces*:*CAIssuers*.

```
      Authority Information Access:
          CA Issuers - URI:http://eqca2017-ca1.e-szigno.hu/eqca2017.
```

3.3.9 (i) URLs of revocation info or info about revocation

The legal requirement

(i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate;

Implementation of the requirement

This requirement makes it mandatory that the certificate includes one of the following options.

- certificate revocation list availability, and/or
- OCSP access details;
- or, if neither of these is included in the certificate, an indication that no revocation information is available (this is only possible for certificates with a short lifetime of 24 hours or less).

This means that the certificate must include RFC 5280:

- the extension *authorityInfoAccess* with *OCSP* method and a URL as value where the OCSP service is available, and/or
- the extension *cRLDistributionPoints* and a URL as value from where the CRL can be downloaded,
- or, if neither of these is present in the certificate, it must contain the extension *noRevAvail* with *NULL*.

Examination of the requirement in the certificate

Using *openssl*, list the certificate and look for *authorityInfoAcces:OCSP* or *cRLDistributionPoints* or *noRevAvail*.

```
X509v3 CRL Distribution Points:
    Full Name:
  URI:http://eqca2017-crl1.e-szigno.hu/eqca2017.crl

Authority Information Access:
    OCSP - URI:http://eqca2017-ocsp1.e-szigno.hu
```

3.3.10(j) if the keys are generated on a QSCD device, its indication

The legal requirement

(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

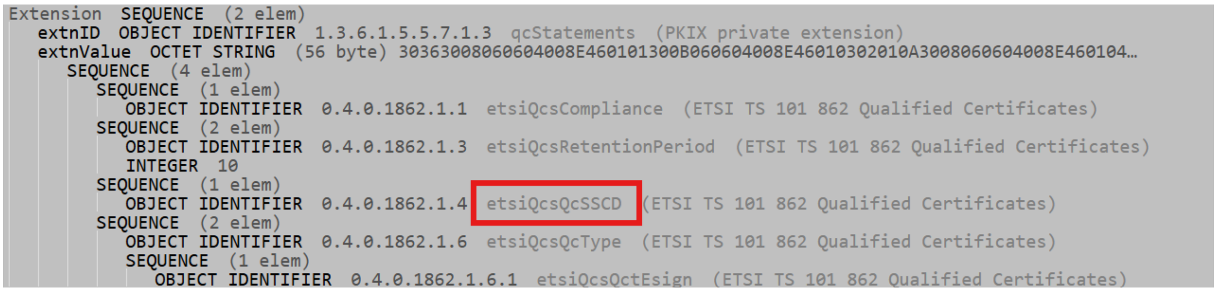
Implementation of the requirement

This requirement makes it mandatory that if the private key for the certificate is generated for a QSCD device, that the certificate contains the *QcSSCD qcStatements* value according to ETSI EN 319412-5.

Examination of the requirement in the certificate

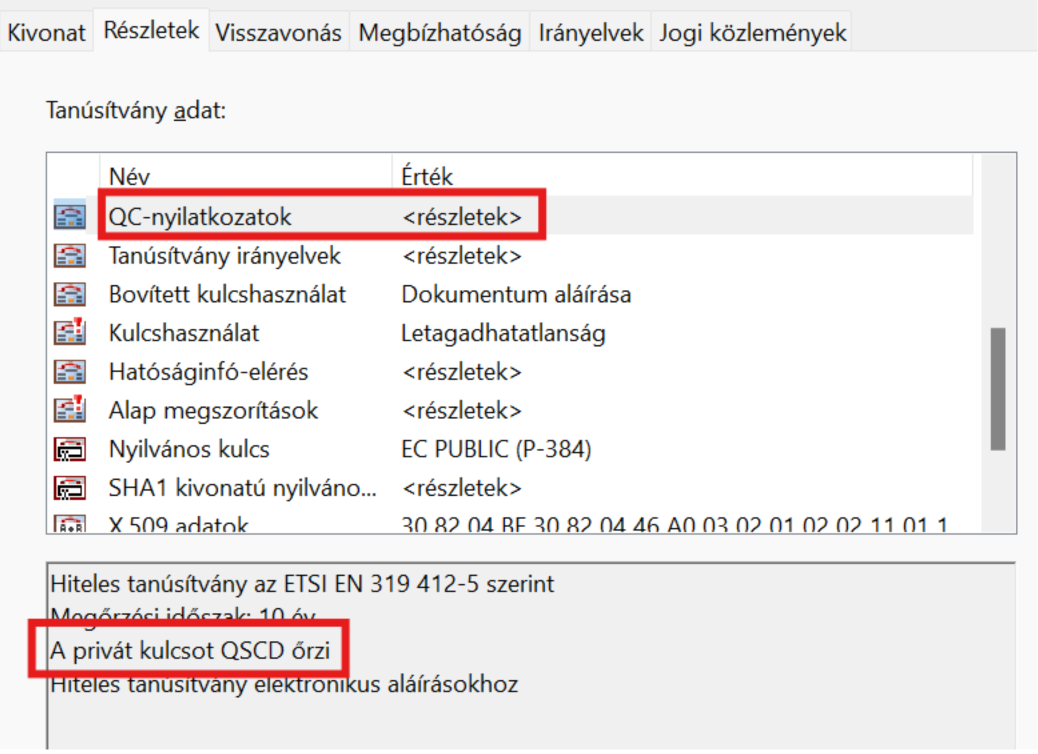
By default, *openssl* does not recognize *qcStatements* extensions, so you can use ASN.1 parser to check.

The ASN.1 structure below shows the *QcSSCD* value.



```
Extension  SEQUENCE  (2 elem)
   extnID  OBJECT IDENTIFIER  1.3.6.1.5.5.7.1.3  qcStatements  (PKIX private extension)
   extnValue  OCTET STRING  (56 byte) 30363008060604008E460101300B060604008E46010302010A3008060604008E460104…
      SEQUENCE  (4 elem)
         SEQUENCE  (1 elem)
            OBJECT IDENTIFIER  0.4.0.1862.1.1  etsiQcsCompliance  (ETSI TS 101 862 Qualified Certificates)
         SEQUENCE  (2 elem)
            OBJECT IDENTIFIER  0.4.0.1862.1.3  etsiQcsRetentionPeriod  (ETSI TS 101 862 Qualified Certificates)
            INTEGER  10
         SEQUENCE  (1 elem)
            OBJECT IDENTIFIER  0.4.0.1862.1.4  etsiQcsQcSSCD  (ETSI TS 101 862 Qualified Certificates)
         SEQUENCE  (2 elem)
            OBJECT IDENTIFIER  0.4.0.1862.1.6  etsiQcsQcType  (ETSI TS 101 862 Qualified Certificates)
            SEQUENCE  (1 elem)
               OBJECT IDENTIFIER  0.4.0.1862.1.6.1  etsiQcsQctEsign  (ETSI TS 101 862 Qualified Certificates)
```

Alternatively, you can view QC statements in Adobe Reader under Certificate details.



Tanúsítvány adat:

Név	Érték
QC-nyilatkozatok	<részletek>
Tanúsítvány irányelvek	<részletek>
Bovített kulcshasználat	Dokumentum aláírása
Kulcshasználat	Letagadhatatlanság
Hatóságinfó-elérés	<részletek>
Alap megszorítások	<részletek>
Nyilvános kulcs	EC PUBLIC (P-384)
SHA1 kivonatú nyilváno...	<részletek>
X.509 adatok	30 82 04 BE 30 82 04 46 A0 03 02 01 02 02 11 01 1

Hiteles tanúsítvány az ETSI EN 319 412-5 szerint
Megőrzési időszak: 10 év
A privát kulcsot QSCD őrzi
Hiteles tanúsítvány elektronikus aláírásokhoz

3.3.11Note on the maximum validity of qualified sign/seal certificates

Several EU Member States have regulations limiting the maximum validity period of certificates, but this is problematic from a legal point of view and should be abolished, as Article 28(2) prohibits the imposition of additional mandatory content requirements for certificates beyond those specified in the relevant Annex.

This legal provision must be reviewed in the Member States following the publication of the Commission's implementing regulations, because with the inclusion of ETSI TS 119 312 among the requirements, there is an EU-level requirement in this regard, so there is no place for Member States to intervene.