A minősített aláírás ellenőrzésének követelményei az eIDAS szerint

V: 1.0

2025-04-04

Tartalom

1 Bevezető

Az alábbi anyag az eIDAS rendelet szerinti minősített elektronikus aláírás ellenőrzésének kérdéseit vizsgálja jogi szemszögből nézve.

Az anyag célja, hogy megállapítsa az általánosan vonatkozó szabályokat a minősített aláírás ellenőrzése kapcsán.

Ez azért szükséges, mert:

- az eIDAS1 keretében nincs kötelezően használandó szabvány
- az eIDAS2 keretében sem várható kötelezően használandó szabvány mert a 32. cikk (1) 2. bekezdése szerint a szabványnak megfelelés esetén **feltételezett**, hogy a jogszabálynak is megfelel a tevékenység.

Ezért mindenféleképpen szükséges bevezetni az **„Article 32 szerinti aláírás ellenőrzés”** fogalmát, mert ez az egy kötelező érvényű ellenőrzési forma mindenkire.

A jogszabály megfelelő pontjainak elemzésével meghatározható/levezethető, hogy milyen elfogadási követelmények vonatkoznak a tanúsítványok tartalmára, a visszavonási információk időbeliségére, az egyes szintek ellenőrzésére.

A következő (2. Összefoglalás) fejezetben összefoglalásra kerültek az értelmezett követelmények, az egyes, pontosító alfejezetekben emellett megtalálhatók a részletes levezetések is.

2 Összefoglalás

Minősített elektronikus aláírás ellenőrzése során az alábbi alfejezetekben található követelmények megvalósulását kell vizsgálni.

2.1 A tanúsítvány tartalmára vonatkozó követelmények

Az aláírói tanúsítványban az alábbi információk kell szerepeljenek:

- Alany (Subject) adatok:
  - *commonName* (CN) – alany neve,
  - *givenName* (GN) – alany keresztneve,
  - *surname* (SN) – alany vezetékneve,
  - *Subject:serialNumber* – az Alany egyediségét biztosító sorszám.

  Megjegyzés: az ETSI EN 319412-2 4.2.4 fejezet előírja az ország (C) feltüntetését, habár kötelezősége nem vezethető le az eIDAS-ból.
- Kiadó (Issuer) adatok
  - *commonName* (CN) – kiadó neve,
  - *organization* (O) – bizalmi szolgáltató nyilvántartás szerinti szervezet neve,
  - *organizationIdentifier* – a bizalmi szolgáltató nyilvántartás szerinti szervezet azonosítója,
  - *countryName* (C) – a bizalmi szolgáltató bejegyzésének országa.
- Tanúsítvány kiterjesztések
  - *authorityInfoAcces:OCSP és/*vagy a *cRLDistributionPoints*
    vagy ezek hiányában a *noRevAvail* kiterjesztés – a visszavonási információk (CRL, OCSP) elérési helyei vagy információ az visszavonási információkról,
  - *qcStatements* kiterjesztéseket:
    - *QcCompliance* – a minősítettség jelzése,
    - *QcType esign* értékkel – a minősített aláíró tanúsítvány jelzése,
    - *QcSSCD* – amennyiben a tanúsítvány privát kulcsa QSCD eszközre került generálásra, ezt kötelező elhelyezni.
  - *authorityInfoAcces:CAIssuers* – az aláíró tanúsítványt aláíró tanúsítványkiadó tanúsítványának letöltési címe.
- Egyéb tanúsítvány adatok
  - az alany nyilvános kulcsa
  - a tanúsítványkiadó aláírása a tanúsítványon
  - a tanúsítvány érvényessége

2.2 Az aláírás szintekre vonatkozó követelmények

Az egyes aláírási szintekre vonatkozó ellenőrizhetőségi követelmények az alábbi táblázatban kerülnek összefoglalásra.

Szint	Szint tartalma	Magyarázat	Tartós megőrzésre alkalmas?	Kiegészítő információ beszerzése szükséges az ellenőrzéshez?	Az aláírás érvényesség megállapíthatósága
B	csak aláírás	Mivel ezen szint esetén sem időbélyeg, sem visszavonási információ nem szerepel az aláírásban, ezért az aláírás érvényessége alaphelyzetben nem állapítható meg.	Nem.	Igen, CRL vagy OCSP válasz beszerzése szükséges.	**Önállóan:** Nem megállapítható. **Beszerzett kiegészítő információkkal:** Az aláíró tanúsítvány (és annak lánca) érvényességi idején belül.
T	aláírás időbélyeggel	Mivel az időbélyeg ezen szinten hiteles információt ad az aláírás időpontjáról, ezért az aláírás érvényessége az időbélyegző tanúsítvány (és annak lánca) érvényességi idején belül állapítható meg.	Nem.	Igen, CRL vagy OCSP válasz beszerzése szükséges.	**Önállóan:** Nem megállapítható. **Beszerzett kiegészítő információkkal:** Az időbélyegző tanúsítvány (és annak lánca) érvényességi idején belül. (Az időbélyegző tanúsítvány jellemzően sokkal tovább érvényes, mint az aláíró.)

Szint	Szint tartalma	Magyarázat	Tartós megőrzésre alkalmas?	Kiegészítő információ beszerzése szükséges az ellenőrzéshez?	Az aláírás érvényesség megállapíthatósága
LT	aláírás időbélyeggel és azt követően csatolt visszavonási információval	Mivel a csatolt visszavonási információt nem védi időbélyeg (azaz kvázi B szinten aláírt információként kerül csatolásra) ezért annak maximum elfogadási ideje a B aláírás szint alapján állapítandó meg.	Nem.	Nem. Amennyiben a CRL vagy OCSP válasz érvényessége lejárt, új CRL vagy OCSP válasz beszerzése szükséges.	**Önállóan:** A visszavonási információ (és annak lánca) érvényességi idején belül. **Beszerzett kiegészítő információkkal:** Az időbélyegző tanúsítvány (és annak lánca) és a visszavonási információ (és annak lánca) érvényességi idején belül.
LTA	aláírás időbélyeggel és visszavonási információval, majd archív időbélyeg	Az archív időbélyeg az összes alatta található tartalmat védi, így azok érvényessége egészen addig megállapítható, amíg a legkülső archív időbélyeg (és annak lánca) érvényességi idején belül történik az ellenőrzés.	Igen	Nem.	Az archív időbélyegző tanúsítvány (és annak lánca) érvényességi idején belül.

2.3 Bizalmi listára vonatkozó követelmények

- A bizalmi listán minősített tanúsítvány kiadójának szerepelnie kell „granted” státusszal az aláíró tanúsítvány kiadásának időpontjában és az aláírás időpontjában.
- A bizalmi listán található láncelem visszavonási állapotát már nem kell ellenőrizni.

2.4 A visszavonási információkra vonatkozó követelmények

- A visszavonási információnak (CRL vagy OCSP válasz) az aláírás időpontját követőnek kell lennie (grace period), azaz mind a CRL, mind az OCSP válasz az aláírás időpontját követően kerül aláírásra/kibocsátásra a bizalmi szolgáltató által. (A CRL, OCSP válasz *thisUpdate* értéke későbbi, mint az aláírás időpontja.)
- A visszavonási információ, amennyiben nem tartalmaz ArchiveCutoff (OCSP) vagy ExpiredCertsOnCRL (CRL) kiegészítést, csak a tanúsítvány érvényességi idején belül fogadható el.

2.5 A certificatePolicies:userNotice:Explicit text mező megjelenítésére vonatkozó követelmény

- Amennyiben a tanúsítvány *certificatePolicies:userNotice:Explicit text* mezőt nem tartalmaz, a tanúsítvány nem rendelkezik explicit korlátozásokkal, az aláírás ellenőrzése tovább haladhat.
- Amennyien nem üres, annak tartalmát az ellenőrzés során az ellenőrző félnek meg kell jeleníteni, hogy elbírálhassa a korlátozásokat és dönthessen az aláírás elfogadásáról.

3 Részletes kifejtés

Az alábbi alfejezetek a 32. cikk és az abból hivatkozott 26. cikk és I. melléklet jogi követelményeit elemzik.

A 32. cikkről szóló részben összefoglaljuk a hivatkozott fejezetek tartalmát a megfelelő helyen, azok részletes kifejtése a saját fejezetükben történik.

3.1 eIDAS 32. cikk

Az eIDAS rendelet a minősített aláírások érvényesítésére vonatkozó szabályokról a 32. cikk (1) bekezdésében rendelkezik, az annak megfelelően ellenőrzött aláírás tekinthető érvényes aláírásnak.

Az alábbi alfejezetek az egyes követelményeket fejtik ki.

3.1.1 (a) az aláíró tanúsítványa megfelel az I. melléklet követelményeinek

A jogi követelmény

a) az aláírást igazoló tanúsítvány az aláírás időpontjában elektronikus aláírás olyan minősített tanúsítványa volt, amely megfelel az I. mellékletnek;

A követelmény megvalósulása

A követelmény röviden azt jelenti, hogy a minősített aláírói tanúsítványnak tartalmaznia kell a következő elemeket:

- Alany (*Subject*) adatok:
  - *commonName* (CN) – alany neve,
  - *givenName* (GN) – alany keresztneve,
  - *surname* (SN) – alany vezetékneve,
  - *Subject:serialNumber* – az Alany egyediségét biztosító sorszám.

  Megjegyzés: az ETSI EN 319412-2 4.2.4 fejezet előírja az ország (C) feltüntetését, habár kötelezősége nem vezethető le az eIDAS-ból.
- Kiadó (*Issuer*) adatok
  - *commonName* (CN) – kiadó neve,
  - *organization* (O) – bizalmi szolgáltató nyilvántartás szerinti szervezet neve,
  - *organizationIdentifier* – a bizalmi szolgáltató nyilvántartás szerinti szervezet azonosítója,
  - *countryName* (C) – a bizalmi szolgáltató bejegyzésének országa.
- Tanúsítvány kiterjesztések
  - *authorityInfoAcces:OCSP és/*vagy a *cRLDistributionPoints*
    vagy ezek hiányában a *noRevAvail* kiterjesztés – a visszavonási információk (CRL, OCSP) elérési helyei, vagy információ a visszavonási információról
  - *qcStatements* kiterjesztéseket:
    - *QcCompliance* – a minősítettség jelzése,
    - *QcType esign* értékkel – a minősített aláíró tanúsítvány jelzése,
    - *QcSSCD* – amennyiben a tanúsítvány privát kulcsa QSCD eszközre került generálásra, ezt kötelező elhelyezni.
  - *authorityInfoAcces:CAIssuers* – az aláíró tanúsítványt aláíró tanúsítványkiadó tanúsítványának letöltési címe.

- Egyéb tanúsítvány adatok
  - az alany nyilvános kulcsa
  - a tanúsítványkiadó aláírása a tanúsítványon
  - a tanúsítvány érvényessége

Az egyes elemek kötelezőségének részletes levezetését az **3.3 eIDAS I. melléklet – a minősített aláíró tanúsítvány** tartalma fejezet tartalmazza.

3.1.2 (b) a tanúsítványt minősített bizalmi szolgáltató bocsátotta ki, és az az aláírás időpontjában érvényes volt

A jogi követelmény

b) a minősített tanúsítványt minősített bizalmi szolgáltató bocsátotta ki, és az az aláírás időpontjában érvényes volt;

Ez tulajdonképpen két fő részkövetelmény, ami további alkövetelményekre bontható:

i. a minősített tanúsítványkiadó ellenőrzése az EU bizalmi listán
ii. annak ellenőrzése, hogy a tanúsítvány az aláírás időpontjában érvényes volt, azaz:
    a. az aláírás az aláíró tanúsítvány érvényességi idején belül történt: (notBefore, notAfter)
    b. az aláírás időpontjában az aláíró tanúsítvány nem volt visszavonva.
    c. a visszavonási információ ellenőrzése, hogy tartalmazhat-e státusz információt az ellenőrzött tanúsítványra vonatkozóan.

A követelmény megvalósulása

Az egyes részkövetelményeket külön-külön tudjuk ellenőrizni.

i. a minősített tanúsítványkiadó ellenőrzése az EU bizalmi listán úgy kell történjen, hogy az aláírás ellenőrzése során meg kell győződni arról, hogy a kibocsátó bizalmi szolgáltató tanúsítványa az aláíró tanúsítvány kibocsátásakor a bizalmi listán „granted” bejegyzéssel szerepelt, továbbá az aláírás időpontjában az nem „withdrawn” állapotú.
ii. Az aláíró tanúsítvány érvényességének ellenőrzése az aláírás időpontjára:
    a. az aláírás időpontjának az aláíró tanúsítvány notBefore és notAfter határai közé kell esnie
    b. **az aláírás időpontját követően kiadott OCSP vagy CRL** válasz szerint a tanúsítvány **nincs visszavonva**. Az aláírás időpontja utáni CRL vagy OCSP válasz azért szükséges, mert az aláírás előtti CRL vagy OCSP válasz még nem tartalmazhat információt a tanúsítvány visszavonásáról/felfüggesztéséről adott időpontban, azt csak **az aláírást követően kibocsátott visszavonási információ biztosíthatja**. (A ETSI TS 119 172-4 szabvány szerinti RevocationFreshnessConstraints maximum értéke tehát 0 lehet.)

       A tanúsítvány akkor **nincs visszavonva**, ha sorozatszáma **a CRL-en nem szerepel**, az OCSP válasz meg „**good**” státuszt mutat.

       Megjegyzés: az Adobe Reader, különösen a beágyazott visszavonási információk esetében azt vizsgálja, hogy a CRL vagy OCSP válasz érvényességén belül esik-e az aláírás. Ez helytelen, mert az előbb leírt okokból lehet olyan, hogy az adott tanúsítvány visszavont állapota még nem szerepel az aláírást megelőzően kiadott CRL-en vagy OCSP válaszban. Ezért fordulhat elő, hogy egy aláírás érvényességét az Adobe Reader érvényesnek mutathatja még akkor is, ha az aláírói tanúsítvány az aláírás előtt vissza lett vonva.

c. annak ellenőrzése, hogy az aláíró tanúsítvány visszavonási információja a tanúsítvány érvényességi idejében került-e kibocsátásra vagy tartalmazza az ArchiveCutoff (OCSP) vagy ExpiredCertsOnCRL (CRL) kiterjesztést.
Ez azért szükséges, mert az RFC 5280 szerint a tanúsítványra csak érvényességi időn belül kell megfelelő státuszt adni, kivéve, ha az tartalmazza a fenti jelzést, mert az azt jelenti, hogy a listáról állapot nem kerül eltávolításra.

Megjegyzés: Az eIDAS 24. cikk (4) szerint ennek az információnak – legalább tanúsítványonként – megbízható, ingyenes és hatékony automatizált formában bármikor, a tanúsítvány érvényességi idejének lejártát követően is elérhetőnek kell lennie., így minősített tanúsítványok esetében az ArchiveCutoff és ExpiredCertsOnCRL kiterjesztések használata kötelező.

Az aláírás érvényességének ellenőrzéséhez a tanúsítványláncban szereplő többi tanúsítvány érvényességét is ellenőrizni kell, melyre a fenti metódust rekurzívan kell alkalmazni.

A követelmények ellenőrzése online, tanúsítványokban, valamint CRL és OCSP válaszokban

i. Bizalmi lista ellenőrzése - A szolgáltatói tanúsítványokat célszerű automatikusan EUTL alapján ellenőrizni. Manuálisan ezen az oldalon vizsgálható meg az érvényesség: https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls

ii. Az aláíró tanúsítvány érvényességének ellenőrzése:

a. Az aláíró tanúsítványban található érvényességi időn belül kell esnie az aláírás időpontjának:

```
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. A visszavonás ellenőrzése:

CRL esetén ennek ellenőrzése:

A visszavonási információ kibocsátási időpontjának (*LastUpdate*) későbbinek kell lennie, mint az aláírás időpontja, és az ellenőrzendő tanúsítvány sorszáma nem szerepelhet rajta.

```
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
```

OCSP esetén ennek ellenőrzése:

A visszavonási információ kibocsátási időpontjának (*ThisUpdate*) későbbinek kell lennie, mint az aláírás időpontja, és az ellenőrzendő tanúsítvány státusza „good” kell legyen.

```
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. Az *ExpiredCertsOnCRL* (CRL) vagy az *ArchiveCutoff* (OCSP) kiterjesztés ellenőrzése a visszavonási információban:

CRL esetén:

Az *openssl* alapértelmezetten nem ismeri az ExpiredCertsOnCRL CRL kiterjesztést, így azt OID-dal jeleníti meg. Az openssl kimenetében a *2.5.29.60* OID-et kell keresni. Az *ExpiredCertsOnCRL* kiterjesztéshez kapcsolódó dátumnak az aláírás időpontját megelőző dátumnak kell lennie.

(Ez jellemzően egyébként a CA kibocsátásának időpontja szokott lenni.)

```
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
```

OCSP esetén:

Az openssl ismeri az ArchiveCutoff OCSP válasz így az értelmezhető az OCSP válaszból.

Az openssl kimenetében az *OCSP Archive Cutoff* kiterjesztést kell keresni. Az *OCSP Archive Cutoff* kiterjesztéshez kapcsolódó dátumnak az aláírás időpontját megelőző dátumnak kell lennie.

(Ez jellemzően egyébként a CA kibocsátásának időpontja szokott lenni.)

```
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 az egyes aláírás szintek érvényessége

Mivel a követelmény az aláírás ellenőrzése során annak érvényességének megállapítása, az egyes aláírás szintek esetében foglalkozni kell azzal is, hogy azok milyen feltételek fennállása esetén ellenőrizhetők sikeresen.

A következő táblázat ezt foglalja össze. Az ezen határokon kívül eső esetekben a 32. cikk szerinti aláírás érvényesség nem állapítható meg.

Szint	**Szint tartalma**	**Magyarázat**	**Tartós megőrzésre alkalmas?**	**Kiegészítő információ beszerzése szükséges az ellenőrzéshez?**	**Az aláírás érvényesség megállapíthatósága**
B	csak aláírás	Mivel ezen szint esetén sem időbélyeg, sem visszavonási információ nem szerepel az aláírásban, ezért az aláírás érvényessége alaphelyzetben nem állapítható meg.	Nem.	Igen, CRL vagy OCSP válasz beszerzése szükséges.	**Önállóan:** Nem megállapítható. **Beszerzett kiegészítő információkkal:** Az aláíró tanúsítvány (és annak lánca) érvényességi idején belül.
T	aláírás időbélyeggel	Mivel az időbélyeg ezen szinten hiteles információt ad az aláírás időpontjáról, ezért az aláírás érvényessége az időbélyegző tanúsítvány (és annak lánca) érvényességi idején belül állapítható meg.	Nem.	Igen, CRL vagy OCSP válasz beszerzése szükséges.	**Önállóan:** Nem megállapítható. **Beszerzett kiegészítő információkkal:** Az időbélyegző tanúsítvány (és annak lánca) érvényességi idején belül. (Az időbélyegző tanúsítvány jellemzően sokkal tovább érvényes, mint az aláíró.)

Szint	Szint tartalma	Magyarázat	Tartós megőrzésre alkalmas?	Kiegészítő információ beszerzése szükséges az ellenőrzéshez?	Az aláírás érvényesség megállapíthatósága
LT	aláírás időbélyeggel és azt követően csatolt visszavonási információval	Mivel a csatolt visszavonási információt nem védi időbélyeg (azaz kvázi B szinten aláírt információként kerül csatolásra) ezért annak maximum elfogadási ideje a B aláírás szint alapján állapítandó meg.	Nem.	Nem. Amennyiben a CRL vagy OCSP válasz érvényessége lejárt, új CRL vagy OCSP válasz beszerzése szükséges.	**Önállóan:** A visszavonási információ (és annak lánca) érvényességi idején belül. **Beszerzett kiegészítő információkkal:** Az időbélyegző tanúsítvány (és annak lánca) és a visszavonási információ (és annak lánca) érvényességi idején belül.
LTA	aláírás időbélyeggel és visszavonási információval, majd archív időbélyeg	Az archív időbélyeg az összes alatta található tartalmat védi, így azok érvényessége egészen addig megállapítható, amíg a legkülső archív időbélyeg (és annak lánca) érvényességi idején belül történik az ellenőrzés.	Igen	Nem.	Az archív időbélyegző tanúsítvány (és annak lánca) érvényességi idején belül.

3.1.3 (c) az írt alá, akitől az ellenőrző fél várta, és úgy írt alá ahogyan várta

A jogi követelmény

c) az aláírás-érvényesítési adatok megfelelnek a szolgáltatást igénybe vevő fél számára megadott adatoknak;

A követelmény vizsgálata

Az aláíró tanúsítványban szereplő alanyt az ellenőrző félnek össze kell vetni azzal, hogy kitől várja az aláírást. Továbbá **ennek a követelménynek a keretében vizsgálandó** az is, hogy az aláíró tanúsítvány az aláírásra, nem szerepel-e benne olyan **használati korlátozás**, amit megakadályozná a tanúsítvány vagy az aláírás elfogadását.

3.1.3.1 A tanúsítványba foglalt használati korlátozások vizsgálata

A jogi követelmény

(2) Amennyiben a bizalmi szolgáltatók előzetesen megfelelően tájékoztatják az ügyfeleiket az általuk nyújtott szolgáltatások igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők (recognizable), a bizalmi szolgáltatók nem felelősek a szolgáltatások igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért.

A követelmény vizsgálata

Az eIDAS 13. cikk (2) alapján, hogy amennyiben a bizalmi szolgáltatásra korlátozások vonatkoznak, a bizalmi szolgáltató felelőssége a korlátozások kapcsán csak akkor zárható ki, ha ezek a korlátozások harmadik felek számára megismerhetők, ezért ezen korlátozások a tanúsítványba kerülnek elhelyezésre.

Az ilyen korlátozások lehetnek:

- Tanúsítvány használatára vonatkozó korlátozások
- Kulcshasználatra vonatkozó korlátozások

3.1.3.1.1 Tanúsítvány használati korlátozás

A követelmény vizsgálata

A tanúsítvány használatára vonatkozó egyedi korlátozások jellemzően szövegszerű korlátozások, amelynek beírására helyet a *certificatePolicies:userNotice:Explicit text* mező biztosít.

Amennyiben ez a mező megtalálható a tanúsítványban, akkor az ellenőrzés során az RFC 5280 4.2.1.4 fejezete alapján meg kell jeleníteni a felhasználó számára, és jelezni, hogy az aláírás csak akkor fogadható el, ha fenti mező nem tartalmaz korlátozást az elfogadhatóságra.

A 13. cikk (3) ebben a kérdésben további szabályozási lehetőséget biztosít a tagállamok számára.

Ez Magyarország esetében tiltó rendelkezést tartalmaz, a Dáptv. 101. § (2) értelmében, az aláíró is kötelezett a korlátozások betartására, azzal nem élhet vissza.

3.1.3.1.2 Kulcs használati korlátozás

A követelmény vizsgálata

A kulcs használatának korlátozására használható a *PrivateKeyUsagePeriod* kiterjesztés. Ez aláíró tanúsítványok esetén nem szerepel, de időbélyegző tanúsítványok esetén szerepelhet.

Amennyiben ezt a kiterjesztést tartalmazza egy tanúsítvány, akkor hozzá tartozó kulccsal végzett aláírás csak akkor fogadható el, ha az aláírás időpontja a *PrivateKeyUsagePeriod* kiterjesztésbe foglalt időtartamon belül készült. Ez időbélyegzők esetében azt jelenti, hogy az időbélyeg akkor érvényes, ha ezen időtartamon belül készült.

A követelmény vizsgálata a tanúsítványban

Az openssl kimenetében keressük meg a *Private Key Usage Period*-ot. Az aláírás dátumának a befoglalt időtartamon belül kell esnie.

```
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) az ellenőrző fél megkapja a tanúsítványt, ami egyedileg azonosítja az aláírót

A jogi követelmény

d) a szolgáltatást igénybe vevő fél pontosan megkapja a tanúsítványban az aláírót azonosító egyedi adatokat;

A követelmény vizsgálata

Az aláíráskonténerbe (formátumba) ágyazott aláíró tanúsítvány teljesíti ezt a követelményt, így PADES, XADES, CADES, ASIC aláírás formátumot használva ez a követelmény biztosan teljesül.

*Az egyediség kapcsán lásd még a **3.2.3 Subject:serialNumber, a 26. cikk 1. (a) és (b) implicit követelménye** fejezetet.*

3.1.5 (e) az álneves tanúsítvány egyértelműen jelölt

A jogi követelmény

e) amennyiben az aláírás időpontjában álnév használatára került sor, az álnév használatának tényét egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;

A követelmény vizsgálata

Egy álneves tanúsítványban az álnevet a *pseudonym* mezőbe kell feltüntetni, amivel az egyértelműen jelölt az ellenőrző fél számára.

Ha a tanúsítvány Alany (Subject) szakasza nem tartalmaz *pseudonym* mezőt, az nem álneves tanúsítvány.

3.1.6 (f) az aláírás QSCD eszközzel lett létrehozva

A jogi követelmény

f) az elektronikus aláírást minősített elektronikus aláírást létrehozó eszközzel állították elő;

A követelmény vizsgálata

Amennyiben az aláíró tanúsítvány tartalmazza a qcStatements kiterjesztésben a *QcSSCD qcStatement*-et, akkor az megfelel a követelménynek.

A követelmény vizsgálata a tanúsítványban

Lásd a **3.3.10 (j) amennyiben QSCD eszközre generált a kulcs, annak feltüntetése** fejezetet.

3.1.7 (g) az aláírás nem sérült

A jogi követelmény

g) az aláírt adatok sértetlensége nem került veszélybe;

A követelmény vizsgálata

Amennyiben az aláírás kriptográfiai validálása sikeres és az aláírás algoritmusa használható, akkor teljesül a feltétel.

3.1.8 (h) az aláírás megfelel a 26. cikk (fokozott aláírás) követelményeinek

A jogi követelmény

h) az aláírás időpontjában teljesültek a 26. cikkben foglalt követelmények;

A követelmény vizsgálata

A követelmény ellenőrzéséhez elég csak az aláírás formátumot megvizsgálni:

Amennyiben az aláírás *PADES, XADES, CADES, ASIC* konténer formátumú és *B, T, LT* (és ebből következően *LTA*) szintű, akkor az aláírás a (már hatályon kívül helyezett) 27. cikk (4) alapján hozott (de még hatályos) 2015/1506 bizottsági végrehajtási határozata alapján megfelel a 26. cikkben foglalt követelményeknek.

Mindemellett a következő fejezetben részletesen végig vesszük a 26. cikk előírásait.

3.2 eIDAS 26. cikk

A 26. cikk tartalmazza a fokozott biztonságú aláírás érvényességének kritériumait.

3.2.1 (a) kizárólag az aláíróhoz köthető

A jogi követelmény

a) kizárólag az aláíróhoz köthető; *((a) it is uniquely linked to the signatory;)*

A követelmény vizsgálata

Az aláíró tanúsítvány tartalma, amennyiben az legalább az aláíró nevét és *Subject:serialNumber*-t tartalmazza egyértelműen hozzáköti az aláírót az aláírásához, mert más alany nem rendelkezhet ugyanezen tartalmú tanúsítvánnyal.

A követelmény vizsgálata a tanúsítványban

Lásd **3.2.3 Subject:serialNumber, a 26. cikk 1. (a) és (b) implicit követelménye** fejezetben.

3.2.2 (b) az aláíró azonosítására alkalmas

A jogi követelmény

b) alkalmas az aláíró azonosítására *((b) it is capable of identifying the signatory;)*

A követelmény vizsgálata

Az aláíró tanúsítvány tartalma, amennyiben az legalább az aláíró nevét és *Subject:serialNumber*-t tartalmazza alkalmas az aláíró azonosítására.

A követelmény vizsgálata a tanúsítványban

Lásd **3.2.3 Subject:serialNumber, a 26. cikk 1. (a) és (b) implicit követelménye** fejezetben.

3.2.3 Subject:serialNumber, a 26. cikk 1. (a) és (b) implicit követelménye

A jogi követelmény

Lásd előző két fejezetet.

A követelmény vizsgálata

Mivel az I. melléklet alapján csak a név kötelező az aláíró tanúsítványba, de az nem elégséges az egyértelmű azonosításhoz, hiszen nem előírás a személynevekre, hogy egyediek legyenek. Így a 26. cikk 1. (a) és (b) miatt szükséges a minősített aláíró tanúsítványokat egy olyan azonosítóval ellátni, ami biztosítja az alany egyedi azonosíthatóságát.

Ennek helye az ETSI EN 319412-2 4.2.4 fejezet szerint a *Subject:serialNumber* mező.

A követelmény vizsgálata a tanúsítványban

Az *openssl*-lel a tanúsítványt listázva *Subject* mezőjében keressük meg a *serialNumber* mezőt.

```
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) az aláíró adatot nagy valószínűséggel csak az aláíró használhatja

A jogi követelmény

c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;

A követelmény vizsgálata

Mivel minősített aláírás esetében a kulcs QSCD eszközön található, az aktiválásához szükséges információ pedig kizárólag a felhasználó birtokában lehet, a követelmény minősített aláíró tanúsítvány használata esetén teljesül.

3.2.5 (d) az aláírt adatok változása nyomon követhető

A jogi követelmény

d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

A követelmény vizsgálata

Amennyiben az aláírás kriptográfiai validálása sikeres és az aláírás algoritmusa használható, akkor teljesül a feltétel.

3.3 eIDAS I. melléklet – a minősített aláíró tanúsítvány tartalma

Az I. melléklet a minősített tanúsítványok tartalmára vonatkozóan az a)-j) pontokban határozza meg a követelményeket.

Az alábbi ezeket vesszük végig, ismertetve a követelményt, annak értelmezését és példákat mutatva az ellenőrzésére.

Az ellenőrzés során az openssl kimeneteket mutatjuk a példákban, ahol értelmezett.

3.3.1 (a) minősített aláíró tanúsítvány jelzése automatizált formában

A jogi követelmény

a) legalább automatizált feldolgozásra alkalmas formában utalnia kell arra, hogy a tanúsítványt elektronikus aláírás minősített tanúsítványaként bocsátották ki;

A követelmény megvalósulása

A tanúsítványban szerepelnie kell a következő ETSI EN 319412-5 szerinti *qcStatements* kiterjesztéseknek:

- *QcCompliance*
  Ennek jelentése, aláíró tanúsítványál, hogy a tanúsítvány az I. melléklet szerint lett kiadva *(bélyegző esetén II.; QWAC esetén IV.)*
- *QcType*
  Ez határozza meg a tanúsítvány típusát, aminek minősített aláírás esetén **esign** értékkel kell rendelkeznie. *(bélyegző esetén eseal)*

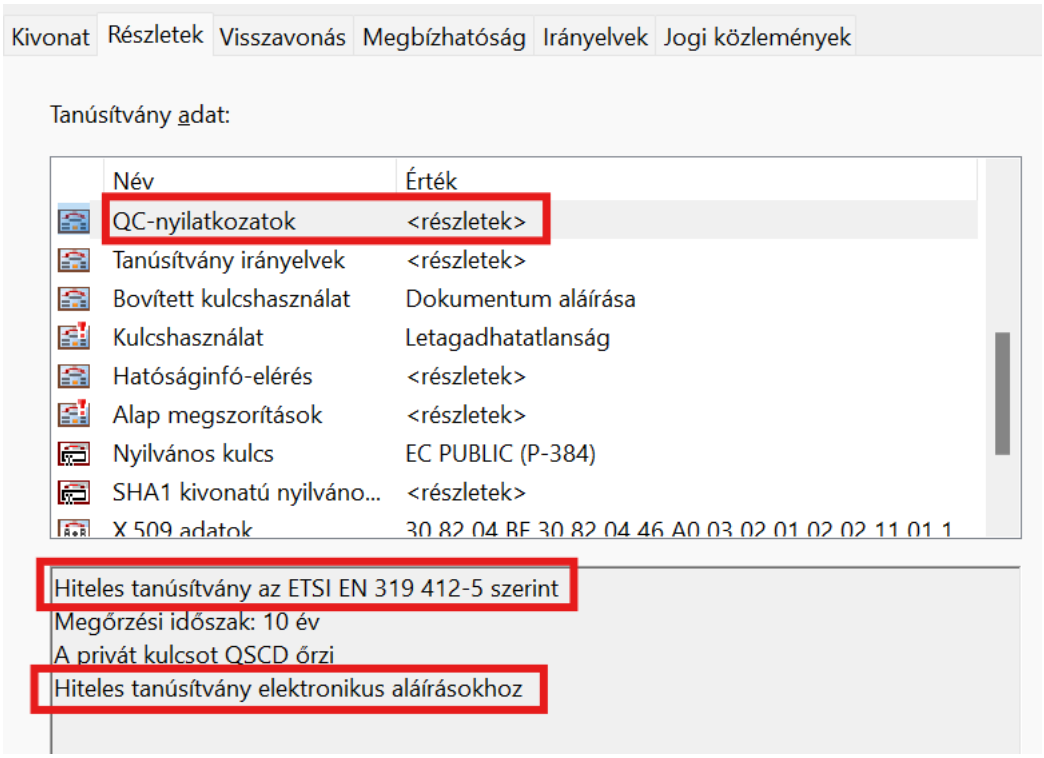
A követelmény vizsgálata a tanúsítványban

Az *openssl* alapértelmezetten nem ismeri a *qcStatements* kiterjesztéseket, így az ellenőrzésre ASN.1 elemzőt használhatunk.

Az alábbi ASN.1 struktúrában látható a *QcCompliance* és a *QcType esign* érték.

```
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 8E460101300B060604008E46010302010A3008060604008E460104…
      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)
```

Másik lehetőség az Adobe Reader-ben a tanúsítvány részletei alatt a QC-nyilatkozatok megtekintése.



3.3.2 (b) a minősített szolgáltatót azonosító adatok

A jogi követelmény

b) a minősített tanúsítványt kibocsátó minősített bizalmi szolgáltatót egyértelműen azonosító adatok, beleértve legalább azt a tagállamot, amelyben az érintett szolgáltató letelepedett, valamint — jogi személy esetében a hivatalos nyilvántartásban szereplő megnevezést és adott esetben nyilvántartási számot,

A követelmény megvalósulása

A tanúsítványban a Kiadó (Issuer) mezőben szerepelnie kell a szolgáltatót minimum azonosító adatoknak. Ezek az ETSI EN 319 412-2 szerint:

- *Organization* – a szolgáltató szervezet nyilvántartás szerinti neve,
- *OrganizationIdentifier* – a szolgáltató nyilvántartás szerinti azonosítója,
- *commonName* – a szolgáltató azon neve, ami magára hivatkozik.

A követelmény vizsgálata a tanúsítványban

Az *openssl*-lel a tanúsítványt listázva *Issuer* mezőjében keressük meg a *C, O, organizationIdentifier* és *CN* mezőket.

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

3.3.3 (c) az alanyt azonosító adatok

A jogi követelmény

c) legalább az aláíró neve vagy pedig egy álnév; álnév használata esetén ezt egyértelműen jelezni kell;

A követelmény megvalósulása

A tanúsítványban az Alany (Subject) mezőben szerepelnie kell a személyt azonosító adatoknak.

- *commonName* – az alany azon neve, ami magára hivatkozik,
- *givenName* – az alany keresztneve,
- *surname* – az alany családneve,
- *Subject:serialNumber* – olyan egyedi azonosító szám, ami lehetővé teszi az egyén egyértelmű azonosítását, mivel az alany neve a névegyezések miatt nem elég az egyedi azonosításhoz. Az azonosító lehet akár egy szolgáltató által képzett azonosító, vagy akár egy egyedi igazolványszám.

Megjegyzés: az ETSI EN 319412-2 4.2.4 fejezet előírja az ország (C) feltüntetését, habár kötelezősége nem vezethető le az eIDAS-ból.

Álneves tanúsítvány esetén (amit gyakorlatilag senki nem igényel) az álnév a *Subject:pseudonym* mezőbe kell kerüljön, ami így egyértelműen jelzi is a tanúsítvány álnevességét.

A követelmény vizsgálata a tanúsítványban

Az *openssl*-lel a tanúsítványt listázva *Subject* mezőjében keressük meg a *CN, GN, SN,* és *serialNumber* mezőket.

```
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) a minősített aláírás érvényesítéséhez használt adat

A jogi követelmény

d) az elektronikus aláírás érvényesítéséhez használt adat, amely megfelel az elektronikus aláírás létrehozásához használt adatnak;

A követelmény megvalósulása

Ez a követelmény a **nyilvános kulcsot** írja elő a tanúsítvány kötelező részének.

Ez azt jelenti, hogy a tanúsítványnak tartalmaznia kell az *RFC 5280* szerinti *SubjectPublicKeyInfo* részt.

A követelmény vizsgálata a tanúsítványban

Az *openssl*-lel a tanúsítványt listázva keressük meg a *SubjectPublicKeyInfo* szakaszt.

Ez RSA és ECC kulcsok esetében eltér, az alábbiakban a minta egy NIST P-256 görbés ECC nyilvános kulcsot mutat.

```
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) a tanúsítvány érvényességi ideje

A jogi követelmény

e) a tanúsítvány érvényességi idejének kezdete és vége;

A követelmény megvalósulása

Ez a követelmény a tanúsítvány érvényességi idejét írja elő a tanúsítvány kötelező részének. Ez azt jelenti, hogy a tanúsítványnak tartalmaznia kell az *RFC 5280* szerinti *notBefore* és *notAfter* értékeket.

A követelmény vizsgálata a tanúsítványban

Az *openssl*-lel a tanúsítványt listázva keressük meg a *notBefore* és *notAfter* értékeket.

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

3.3.6 (f) a tanúsítvány szolgáltatóra egyedi azonosító kódja

A jogi követelmény

f) a tanúsítvány azonosító kódja, amelynek a minősített bizalmi szolgáltatóhoz tartozó egyedi kódnak kell lennie;

A követelmény megvalósulása

A követelmény első felét a tanúsítvány *Certificate:serialNumber* mezője valósítja meg. Ahhoz, hogy a követelmény második fele teljesüljön, miszerint a szolgáltatóra egyedi legyen, az ETSI EN 319411-1 GEN-6.3.3-02A követelmény betartása szükséges, miszerint az tanúsítvány sorozatszáma tartalmazzon véletlent.

A követelmény vizsgálata a tanúsítványban

Az *openssl*-lel a tanúsítványt listázva keressük meg a Certificate alatt Serial Number bejegyzést

```
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) a bizalmi szolgáltató aláírása

A jogi követelmény

g) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírása vagy fokozott biztonságú elektronikus bélyegzője;

A követelmény megvalósulása

Ez a követelmény a szolgáltató aláírását írja elő a tanúsítvány kötelező részének.

Ez azt jelenti, hogy a tanúsítványnak tartalmaznia kell az *RFC 5280* szerinti *Signature Algorithm* és *Signature Value* értékeket.

A követelmény vizsgálata a tanúsítványban

Az *openssl*-lel a tanúsítványt listázva keressük meg a `Signature Algorithm` és `Signature Value` értékeket.

```
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) a kiadói tanúsítvány letöltési URL-je

A jogi követelmény

h) az a helyszín, ahol a g) pontban említett, a fokozott biztonságú elektronikus aláírásra vagy fokozott biztonságú elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;

A követelmény megvalósulása

Ez a követelmény kötelezővé teszi, hogy a tanúsítvány magába foglaljon egy olyan URL-t, ahol letölthető a tanúsítványt kiadó tanúsítvány.

Ez azt jelenti, hogy a tanúsítványnak tartalmaznia kell az *RFC 5280* szerinti *authorityInfoAccess* kiterjesztést *CAIssuers* metódussal, és egy URL-t értékként, ahol a tanúsítvány letölthető.

A követelmény vizsgálata a tanúsítványban

Az *openssl*-lel a tanúsítványt listázva keressük meg az *authorityInfoAcces:CAIssuers* értékeket.

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

3.3.9 (i) a visszavonási nyilvántartások elérhetőségei

A jogi követelmény

i) információ a minősített tanúsítvány érvényességi állapotáról, vagy azoknak a szolgáltatásoknak a helye, amelyek segítségével arról felvilágosítás kérhető;

A követelmény megvalósulása

Ez a követelmény kötelezővé teszi, hogy a tanúsítvány magába foglalja a következő lehetőségek valamelyikét.

- tanúsítvány visszavonási lista elérhetőség, és/vagy
- OCSP elérhetőség;
- vagy ha ezek egyike sem található meg a tanúsítványban, annak jelzését, hogy nincs visszavonási információ (ez kizárólag rövid élettartamú, max. 24 órás érvényességű tanúsítványok esetén lehetséges).

Ez azt jelenti, hogy a tanúsítványnak tartalmaznia kell az *RFC 5280* szerint:

- az *authorityInfoAccess* kiterjesztést *OCSP* metódussal, és egy URL-t értékként, ahol az OCSP szolgáltatás elérhető, és/vagy
- a *cRLDistributionPoints* kiterjesztést és egy URL-t értékként, ahonnan a CRL letölthető,
- vagy ha ezek egyike sem található meg a tanúsítványban akkor tartalmaznia kell a *noRevAvail* kiterjesztést NULL értékkel.

A követelmény vizsgálata a tanúsítványban

Az *openssl*-lel a tanúsítványt listázva keressük meg az *authorityInfoAcces:OCSP* vagy a *cRLDistributionPoints* vagy a *noRevAvail* értékeket.

```
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) amennyiben QSCD eszközre generált a kulcs, annak feltüntetése

A jogi követelmény

j) amennyiben az elektronikus aláírás érvényesítéséhez használt adathoz kapcsolódó, elektronikus aláírás létrehozásához használt adat minősített elektronikus aláírást létrehozó eszközön található, ennek megfelelő feltüntetése, legalább automatizált feldolgozásra alkalmas formában.

A követelmény megvalósulása

Ez a követelmény kötelezővé teszi, hogy amennyiben a tanúsítványhoz tartozó privát kulcs QSCD eszközre került generálásra, hogy a tanúsítvány tartalmazza az ETSI EN 319412-5 szerinti *QcSSCD qcStatements* értéket.

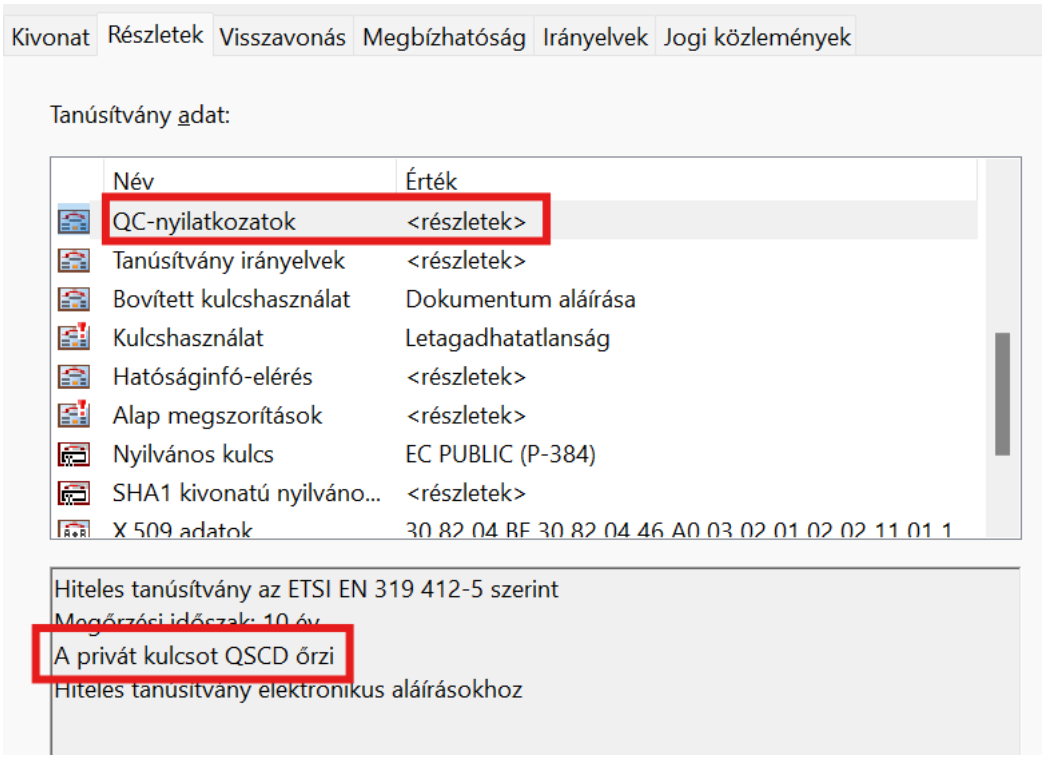
A követelmény vizsgálata a tanúsítványban

Az *openssl* alapértelmezetten nem ismeri a *qcStatements* kiterjesztéseket, így az ellenőrzésre ASN.1 elemzőt használhatunk.

Az alábbi ASN.1 struktúrában látható a *QcSSCD* érték.

```
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)
```

Másik lehetőség az Adobe Reader-ben a tanúsítvány részletei alatt a QC-nyilatkozatok megtekintése.



3.3.11 Megjegyzés az aláíró/bélyegző tanúsítványok maximum érvényességével kapcsolatosan

Számos EU tagállamban létezik olyan szabályozás, amely a tanúsítvány maximális élettartamát korlátozza, azonban ez jogi szempontból problémás, ezt az előírást törölni kellene, mert a 28. cikk 2. paragrafus tiltja a tanúsítványra vonatkozó további kötelező tartalom előírását, mint amit a vonatkozó Melléklet előír.

Ez a jogi szakasz a tagállamokban a bizottsági végrehajtási rendeletek kihirdetését követően mindenképpen felülvizsgálatra kell kerüljön, mert az ETSI TS 119 312 beemelésével a követelmények közé, létezik erre vonatkozóan EU szintű követelmény, így tagállaminak nincs helye.