2025/1943

2025.9.30.

A BIZOTTSÁG (EU) 2025/1943 VÉGREHAJTÁSI RENDELETE

(2025. szeptember 29.)

a 910/2014/EU európai parlamenti és tanácsi rendeletnek az elektronikus aláírások minősített tanúsítványaira és az elektronikus bélyegzők minősített tanúsítványaira vonatkozó referenciaszabványok tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 28. cikke (6) bekezdésére és 38. cikke (6) bekezdésére,

mivel:

(1) Az elektronikus aláírások minősített tanúsítványai és az elektronikus bélyegzők minősített tanúsítványai kulcsszerepet töltenek be a digitális üzleti környezetben, elősegítve a hagyományos papíralapú eljárásokról az elektronikus megfelelőikre való átállást. Az elektronikus aláírást érvényesítő adatoknak vagy az elektronikus bélyegzőt érvényesítő adatoknak egy természetes vagy jogi személyhez kapcsolásával, valamint e személy nevének igazolásával a minősített tanúsítványok fokozzák az aláírónak és a bélyegző létrehozójának a személyazonosságával kapcsolatos bizonyosságot.

(2) A 910/2014/EU rendelet 28. cikkének (6) bekezdésében és 38. cikkének (6) bekezdésében előírt megfelelési vélelem csak akkor alkalmazandó, ha az elektronikus aláírások minősített tanúsítványainak kibocsátása céljából nyújtott minősített bizalmi szolgáltatások, valamint az elektronikus bélyegzők minősített tanúsítványainak kibocsátása céljából nyújtott minősített bizalmi szolgáltatások megfelelnek az e rendeletben meghatározott szabványoknak. E szabványoknak tükrözniük kell a bevett gyakorlatokat, és széles körben elismertnek kell lenniük az érintett ágazatokban. A szóban forgó szabványokat ki kell igazítani oly módon, hogy magukban foglaljanak a minősített bizalmi szolgáltatásoknak és a minősített tanúsítványok tartalmának a biztonságát és megbízhatóságát garantáló további ellenőrzéseket.

(3) Ha a bizalmi szolgáltató megfelel az e rendelet mellékletében meghatározott követelményeknek, a felügyeleti szerveknek vélelmezniük kell a 910/2014/EU rendelet vonatkozó követelményeinek való megfelelést, és ezt a vélelmet kellőképpen figyelembe kell venniük a bizalmi szolgáltatás minősített státuszának megadása vagy megerősítése során. A minősített bizalmi szolgáltatók azonban továbbra is alkalmazhatnak más gyakorlatot a 910/2014/EU rendelet követelményeinek való megfelelés igazolásához.

(4) A Bizottság rendszeresen értékel új technológiákat, gyakorlatokat, szabványokat és technikai specifikációkat. Az (EU) 2024/1183 európai parlamenti és tanácsi rendelet ([2]) (75) preambulumbekezdése értelmében a Bizottságnak rendszeresen felül kell vizsgálnia, és szükség esetén aktualizálnia kell ezt a rendeletet, hogy az folyamatosan megfeleljen a globális fejleményeknek, az új technológiáknak, a szabványoknak és a technikai specifikációknak, illetve igazodjon a belső piaci bevált gyakorlatokhoz.

(5) Az e rendelet szerinti személyesadat-kezelési tevékenységre az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([3]) és adott esetben a 2002/58/EK európai parlamenti és tanácsi irányelv ([4]) alkalmazandó.

([1]) HL L 257., 2014.8.28., 73. o., ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról (HL L, 2024/1183, 2024.4.30., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37. o., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(6) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([5]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor az európai adatvédelmi biztossal, aki 2025. június 6-án véleményt nyilvánított.

(7) Az e rendeletben előírt intézkedések összhangban vannak a 910/2014/EU rendelet 48. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

Az elektronikus aláírások és elektronikus bélyegzők minősített tanúsítványaira vonatkozó referenciaszabványok és specifikációk

(1) A 910/2014/EU rendelet 28. cikkének (6) bekezdésében említett referenciaszabványokat és specifikációkat e rendelet I. melléklete tartalmazza.

(2) A 910/2014/EU rendelet 38. cikkének (6) bekezdésében említett referenciaszabványokat és specifikációkat e rendelet II. melléklete tartalmazza.

2. cikk

Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2025. szeptember 29-én.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

([5]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

I. MELLÉKLET

Az elektronikus aláírások minősített tanúsítványaira vonatkozó referenciaszabványok és specifikációk jegyzéke

Az ETSI EN 319 411-2 V2.6.1 (a továbbiakban: ETSI EN 319 411-2), az ETSI EN 319 412-1 V1.6.1 (a továbbiakban: ETSI EN 319 412-1), az ETSI EN 319 412-2 V2.4.1 (a továbbiakban: ETSI EN 319 412-2) és az ETSI EN 319 412-5 V2.5.1 (a továbbiakban: ETSI EN 319 412-5) szabvány alkalmazandó, a következő kiigazításokkal:

1. Az ETSI EN 319 411-2 esetében

1. 2.1. Normatív hivatkozások

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers" (Elektronikus aláírások és bizalmi infrastruktúrák (ESI). Bizalmi szolgáltatókra vonatkozó általános szabályzati rend követelményei).

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements" (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványokat kibocsátó bizalmi szolgáltatókra vonatkozó szabályzati rend és biztonsági követelmények. 1. rész: Általános követelmények), a következő kiigazításokkal:

Az ETSI EN 319 411-1 V1.5.1 szabvány „2.1. Normatív hivatkozások" című szakasza a következőképpen módosul:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) „Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers" (Elektronikus aláírások és bizalmi infrastruktúrák (ESI). Bizalmi szolgáltatókra vonatkozó általános szabályzati rend követelményei).

— [10] ETSI EN 319 412-2 V2.4.1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons" (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványprofilok. 2. rész: Tanúsítványprofil a természetes személyek számára kibocsátott tanúsítványokhoz).

— [14] ETSI EN 319 412-1 V1.6.1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures" (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványprofilok. 1. rész: Áttekintés és közös adatszerkezetek).

— [3] ETSI EN 319 412-5 V2.5.1 „Electronic Signatures and Infrastructures (ESI). Certificate Profiles. Part 5: QCStatements" (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványprofilok. 5. rész: QCStatements).

— [5] ETSI EN 319 412-1 V1.6.1 „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures" (Elektronikus aláírások és bizalmi infrastruktúrák (ESI). Tanúsítványprofilok. 1. rész: Áttekintés és közös adatszerkezetek).

— [6] CEN/TS 419261:2015 „Security requirements for trustworthy systems managing certificates and time-stamps" (A tanúsítványokat és időbélyegeket kezelő megbízható rendszerek biztonsági követelményei).

— [7] Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms" (Elfogadott kriptográfiai mechanizmusok), az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kiadványa ([1]).

— [8] A Bizottság (EU) 2024/482 végrehajtási rendelete ([2]) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról.

— [9] A Bizottság (EU) 2024/3144 végrehajtási rendelete ([3]) az (EU) 2024/482 végrehajtási rendeletnek az alkalmazandó nemzetközi szabványok tekintetében történő módosításáról és az említett végrehajtási rendelet helyesbítéséről.

— [10] ISO/IEC 15408:2022 (1–5. rész): „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security" (Információbiztonság, kiberbiztonság és a magánélet védelme. Az informatikai biztonságértékelés kritériumai).

— [11] FIPS PUB 140-3 (2019) „Security Requirements for Cryptographic Modules" (Kriptográfiai modulok biztonsági követelményei).

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) HL L, 2024/482, 2024.2.7., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) HL L, 2024/3144, 2024.12.19., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2. 5.2. A tanúsítványalkalmazási nyilatkozatra vonatkozó követelmények

— OVR-5.2-02 A bizalmi szolgáltató (TSP) dokumentációjában meghatározott hitelesítési rend(ek) (CP) feltünteti(k) az alkalmazandó tanúsítványprofilokra vonatkozó követelményeket.

3. 5.3 A hitelesítési rend neve és azonosítása

— OVR-5.3-01 Ha a 4.2.2. szakaszban ismertetett CP olyan változtatására kerül sor, amely kihat az alkalmazhatóságra, akkor módosítani kell a hitelesítési rend azonosítóját.

4. 6.1. Közzétételi és adattárral kapcsolatos felelősségi körök

— OVR-6.1-02 Az ETSI EN 319 411-1 szabvány [2] DIS-6.1-04 követelményében meghatározott információk nyilvánosan és nemzetközileg hozzáférhetők.

5. 6.2.2. Kezdeti azonosság-ellenőrzés

— REG-6.2.2-01A Az alany azonosságára vonatkozó attribútumok és bizonyítékok gyűjtése és validálása a 910/2014/EU rendelet [i.1] 24. cikkének (1c) bekezdése alapján elfogadott végrehajtási jogi aktusokban megadottakkal összhangban történik.

— REG-6.2.2-02 [QCP-n] és [QCP-n-qscd] A természetes személy azonosságának és – adott esetben – egyedi attribútumainak ellenőrzése a 910/2014/EU rendelet [i.1] 24. cikkének (1c) bekezdése alapján elfogadott végrehajtási jogi aktusokkal összhangban történik.

— 1. MEGJEGYZÉS érvénytelen.

6. 6.3.3. Tanúsítványkibocsátás

— GEN-6.3.3-01 Az ETSI EN 319 411-1 szabvány [2] 6.3.3. szakaszában meghatározott GEN-6.3.3-01–GEN-6.3.3-10 követelmények alkalmazandók.

— GEN-6.3.3-02 [FELTÉTELES] Ha egy, a jogi személlyel kapcsolatban azonosított természetes személy részére tanúsítványt bocsátanak ki, a tanúsítványban a szervezetet azonosító alanyattribútumok a jogi személyt vagy az adott jogi személy alszervezetét jelölik, a tanúsítványban szereplő alanyazonosító pedig a természetes személynek felel meg.

— GEN-6.3.3-03 A CP azonosítója [VÁLASZTHATÓ]:

a) [QCP-n]

— az 5.3. szakasz a) pontjában meghatározottak szerint, és/vagy

— a TSP, más releváns érdekelt fél vagy más szabványosítási szervezet által az e dokumentumban meghatározott alkalmazandó követelményeket pontosító hitelesítési rendhez kiosztott objektumazonosító (OID);

b) [QCP-n-qscd]

— az 5.3. szakasz c) pontjában meghatározottak szerinti, és/vagy

— a TSP, más releváns érdekelt fél vagy más szabványosítási szervezet által az e dokumentumban meghatározott alkalmazandó követelményeket pontosító hitelesítési rendhez kiosztott objektumazonosító (OID).

7. 6.3.5. Kulcspár- és tanúsítványhasználat

— SDP-6.3.5-02A [FELTÉTELES] Ha a TSP kezeli az alany helyett a minősített aláírást létrehozó eszközt (QSCD), a TSP olyan minősített bizalmi szolgáltató, amely a 910/2014/EU rendelettel [i.1] összhangban távoli minősített elektronikus aláírást létrehozó eszköz kezelésére irányuló minősített bizalmi szolgáltatást nyújt.

— SDP-6.3.5-11A Az előfizető kötelezettségei (lásd a 6.3.4. szakaszt), ha az előfizető vagy az alany létrehozza az alany kulcsait:

a) arra vonatkozó kötelezettség, hogy az alany kulcsait az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [7] megfelelő algoritmus használatával hozzák létre a tanúsított kulcsnak a CP-ben meghatározott felhasználási céljaira;

b) arra vonatkozó kötelezettség, hogy az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [7] megfelelő kulcshosszt és algoritmust használjanak a tanúsítvány érvényességi ideje során a tanúsított kulcsnak a CP-ben meghatározott felhasználási céljaira.

8. 6.3.10. Tanúsítványstátusz-szolgáltatások

— CSS-6.3.10-08 [FELTÉTELES] Ha rendelkezésre áll tanúsítvány-visszavonási lista (CRL), a TSP gondoskodik arról, hogy legalább a CSS-6.3.10-12 pontban előírt tanúsítványalkalmazási nyilatkozatban (CPS) meghatározott ideig megmaradjon az utolsó CRL integritása és rendelkezésre állása.

9. 6.4.4. Személyzeti ellenőrzések

— OVR-6.4.4-02 A TSP bizalmi szerepet betöltő személyzete és adott esetben bizalmi szerepet betöltő alvállalkozói képesek teljesíteni a formális képzés és bizonyítványok, illetve a tényleges szakmai tapasztalat, vagy pedig a kettő kombinációja révén szerzett szaktudásra, tapasztalatra és képesítésre vonatkozó követelményt.

— OVR-6.4.4-03 Az OVR-6.4.4-02 követelmény betartása magában foglalja az új fenyegetésekre és a jelenlegi biztonsági gyakorlatokra vonatkozó rendszeres (legalább 12 havi) tájékoztatást.

— OVR-6.4.4-04 Az ETSI EN 319 401 szabványban [1] (7.2-15. szakasz) meghatározott bizalmi szerepek mellett a TS 419261 szabványban [6] meghatározott felelősségi körökkel rendelkező, nyilvántartásba vételért és visszavonásért felelős tisztviselők bizalmi szerepei is támogatandók. Azokban az esetekben, amikor a minősített bizalmi szolgáltatót (QTSP) egy tagállam vagy közigazgatási szerv közvetlenül irányítja, illetve az utóbbiak nevében más működteti, ezeket a további bizalmi szerepeket a helyi vagy regionális közigazgatásban feladatot ellátó, nyilvántartásba vételért és visszavonásért felelős tisztviselőket helyettesítő és azok nevében eljáró egy vagy több hivatalos képviselő is betöltheti.

10. 6.4.9. Tanúsító vagy nyilvántartó hatóság általi megszüntetés

— OVR-6.4.9-02 A TSP-nek a szolgáltatás megszüntetésére vonatkozó terve megfelel a 910/2014/EU rendelet [i.1] 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusokban meghatározott követelményeknek.

11. 6.5.1. Kulcspárok létrehozása és telepítése

— OVR-6.5.1-01A A tanúsító hatóság (CA) kulcspárjának generálását az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [7] a CA aláírási célja tekintetében megfelelő algoritmus alkalmazásával kell végezni.

— OVR-6.5.1-01B A CA aláírási kulcsához kiválasztott kulcshossz és algoritmus a CA aláírási célja tekintetében megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [7].

— OVR-6.5.1-01C [FELTÉTELES] Ha a CA generálja az alany kulcsait, a CA által létrehozott alanykulcsok a tanúsítvány érvényességi ideje alatt a CP-ben meghatározott célok tekintetében megfelelnek az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [7].

12. 6.5.2. A személyes kulcs védelme és a kriptográfiai modulok műszaki ellenőrzései

— GEN-6.5.2-01 Az ETSI EN 319 411-1 szabvány [2] 6.5.2. szakaszában meghatározott összes követelmény alkalmazandó, az OVR-6.5.2-01, OVR-6.5.2-03 és OVR-6.5.2-04 követelmények kivételével.

— GEN-6.5.2-02 A TSP kulcspárjának generálását – beleértve a visszavonási és nyilvántartásba vételi szolgáltatások által használt kulcsokét is – olyan biztonságos kriptográfiai eszközön belül kell végrehajtani, amely az alábbiaknak megfelelően tanúsított, megbízható rendszer:

— az informatikai biztonságértékelés közös kritériumai az ISO/IEC 15408 szabvány [10] szerint vagy az informatikai biztonságértékelés közös kritériumainak megfelelően, CC:2002 verzió, 1–5. rész, közzétéve az informatikai biztonság területén a közös kritériumokra vonatkozó tanúsítványok elismeréséről szóló megállapodás résztvevői által, EAL 4 vagy magasabb szintű tanúsítással, vagy

— a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) [8][9], EAL 4 vagy magasabb szintű tanúsítással, vagy

— 2030.12.31-ig a FIPS PUB 140-3 szabvány [11] 3. szintje.

A tanúsítás kockázatelemzés alapján, fizikai és egyéb, nem technikai biztonsági intézkedések figyelembevételével történik, olyan biztonsági cél vagy védelmi profil, illetve modulterv- és biztonsági dokumentáció szerint, amely megfelel a jelen dokumentumban szereplő követelményeknek.

Ha a biztonságos kriptográfiai eszköz EUCC [8][9] tanúsítással rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják.

— GEN-6.5.2-03 A CA személyes aláírási kulcsát a GEN-6.5.2-01 és a GEN-6.5.2-02 pont követelményeinek megfelelő biztonságos kriptográfiai eszközön belül tárolják és használják.

13. 6.5.7. Hálózatbiztonsági ellenőrzések

— OVR-6.5.7-02 Az ETSI EN 319 401 szabvány [1] REQ-7.8-13 követelményében előírt sebezhetőségi vizsgálatot negyedévente legalább egyszer elvégzik.

— OVR-6.5.7-03 Az ETSI EN 319 401 szabvány [1] REQ-7.8-17X követelményében előírt behatolási tesztelést évente legalább egyszer elvégzik.

— OVR-6.5.7-04 A tűzfalakat úgy konfigurálják, hogy megakadályozzák a TSP működéséhez nem szükséges protokollok használatát és hozzáférést.

14. 6.6.1. Tanúsítványprofil

— GEN-6.6.1-05 A tanúsítvány tartalmazza a GEN-6.3.3-03 [VÁLASZTHATÓ] pontban meghatározott hitelesítésirend-azonosítók egyikét. A tanúsítvány a TSP által kiosztott más OID-ket is tartalmazhat.

2. Az ETSI EN 319 412-2 esetében

1. 2.1. Normatív hivatkozások

— [2] ETSI EN 319 412-5 V2.5.1 „Electronic Signatures and Infrastructures (ESI). Certificate Profiles. Part 5: QCStatements" (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványprofilok. 5. rész: QCStatements).

— [9] Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms" (Elfogadott kriptográfiai mechanizmusok), az ENISA kiadványa.

2. 4.2.2. Aláírás

— GEN-4.2.2-2 Az aláírási algoritmus kiválasztása az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [9] összhangban történik.

— MEGJEGYZÉS érvénytelen.

3. 4.2.3.1. Jogi személynek minősülő kibocsátók

   — GEN-4.2.3.1-3 Ha ismert megfelelő nyilvántartási szám, akkor a kibocsátó azonosító adataiban szereplő organizationIdentifier értéke a nyilvántartási számot megállapító hivatalos nyilvántartásban feltüntetett nyilvántartási számot tartalmazza.

4. 4.2.5. Az alany nyilvános kulcsának adatai

   — GEN-4.2.5-2 Az alany nyilvános kulcsának kiválasztása az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [9] összhangban történik.

   — MEGJEGYZÉS érvénytelen.

5. 4.2.6. Sorozatszám

   — GEN-4.2.6-01 A tanúsítvány (IETF RFC 5280 szabvány [1] 4.1.2.2. szakaszában meghatározott) serialNumber értéke a TSP által kibocsátott minden egyes tanúsítvány esetében egyedi.

II. MELLÉKLET

Az elektronikus bélyegzők minősített tanúsítványaira vonatkozó referenciaszabványok és specifikációk jegyzéke

Az ETSI EN 319 411-2 V2.6.1 (a továbbiakban: ETSI EN 319 411-2), az ETSI EN 319 412-1 V1.6.1 (a továbbiakban: ETSI EN 319 412-1), az ETSI EN 319 412-3 V1.3.1 (a továbbiakban: ETSI EN 319 412-3), az ETSI EN 319 412-2 V2.4.1 (a továbbiakban: ETSI EN 319 412-2) és az ETSI EN 319 412-5 V2.5.1 (a továbbiakban: ETSI EN 319 412-5) szabvány alkalmazandó, a következő kiigazításokkal:

1. Az ETSI EN 319 411-2 esetében

1. 2.1. Normatív hivatkozások

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers” (Elektronikus aláírások és bizalmi infrastruktúrák (ESI). Bizalmi szolgáltatókra vonatkozó általános szabályzati rend követelményei).

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements” (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványokat kibocsátó bizalmi szolgáltatókra vonatkozó szabályzati rend és biztonsági követelmények. 1. rész: Általános követelmények), a következő kiigazításokkal:

Az ETSI EN 319 411-1 V1.5.1 szabvány „2.1. Normatív hivatkozások” című szakasza a következőképpen módosul:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) „Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers” (Elektronikus aláírások és bizalmi infrastruktúrák (ESI). Bizalmi szolgáltatókra vonatkozó általános szabályzati rend követelményei).

— [10] ETSI EN 319 412-2 V2.4.1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons” (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványprofilok. 2. rész: Tanúsítványprofil a természetes személyek számára kibocsátott tanúsítványokhoz).

— [14] ETSI EN 319 412-1 V1.6.1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures” (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványprofilok. 1. rész: Áttekintés és közös adatszerkezetek).

— [3] ETSI EN 319 412-5 V2.5.1 „Electronic Signatures and Infrastructures (ESI). Certificate Profiles. Part 5: QCStatements” (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványprofilok. 5. rész: QCStatements).

— [5] ETSI EN 319 412-1 V1.6.1 „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures” (Elektronikus aláírások és bizalmi infrastruktúrák (ESI). Tanúsítványprofilok. 1. rész: Áttekintés és közös adatszerkezetek).

— [6] CEN/TS 419261:2015 „Security requirements for trustworthy systems managing certificates and time-stamps” (A tanúsítványokat és időbélyegeket kezelő megbízható rendszerek – CEN által kidolgozott – biztonsági követelményei).

— [7] Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms” (Elfogadott kriptográfiai mechanizmusok), az ENISA kiadványa.

— [8] Az (EU) 2024/482 végrehajtási rendelet a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról.

— [9] Az (EU) 2024/3144 végrehajtási rendelet az (EU) 2024/482 végrehajtási rendeletnek az alkalmazandó nemzetközi szabványok tekintetében történő módosításáról és az említett végrehajtási rendelet helyesbítéséről.

— [10] ISO/IEC 15408:2022 (1–5. rész) „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security” (Információbiztonság, kiberbiztonság és a magánélet védelme. Az informatikai biztonságértékelés kritériumai).

— [11] FIPS PUB 140-3 (2019) „Security Requirements for Cryptographic Modules” (Kriptográfiai modulok biztonsági követelményei).

2. 5.2. A tanúsítványalkalmazási nyilatkozatra vonatkozó követelmények

— OVR-5.2-02 A bizalmi szolgáltató (TSP) dokumentációjában meghatározott hitelesítési rend(ek) (CP) feltünteti(k) az alkalmazandó tanúsítványprofilokra vonatkozó követelményeket.

3. 5.3 A hitelesítési rend neve és azonosítása

— OVR-5.3-01 Ha a 4.2.2. szakaszban ismertetett CP olyan változtatására kerül sor, amely kihat az alkalmazhatóságra, akkor módosítani kell a hitelesítési rend azonosítóját.

4. 6.1. Közzétételi és adattárral kapcsolatos felelősségi körök

— OVR-6.1-02 Az ETSI EN 319 411-1 szabvány [2] DIS-6.1-04 követelményében meghatározott információk nyilvánosan és nemzetközileg hozzáférhetők.

5. 6.2.2. Kezdeti azonosság-ellenőrzés

— REG-6.2.2-01A Az alany azonosságára vonatkozó attribútumok és bizonyítékok gyűjtése és validálása a 910/2014/EU rendelet [i.1] 24. cikkének (1c) bekezdése alapján elfogadott végrehajtási jogi aktusokban megadottakkal összhangban történik.

— REG-6.2.2-03 [QCP-l] és [QCP-l-qscd] A jogi személy azonosságának és – adott esetben – egyedi attribútumainak ellenőrzése a 910/2014/EU rendelet [i.1] 24. cikkének (1c) bekezdése alapján elfogadott végrehajtási jogi aktusokkal összhangban történik.

— 3. MEGJEGYZÉS Lásd a 2. megjegyzést.

6. 6.3.3. Tanúsítványkibocsátás

— GEN-6.3.3-01 Az ETSI EN 319 411-1 szabvány [2] 6.3.3. szakaszában meghatározott GEN-6.3.3-01–GEN-6.3.3-10 követelmények alkalmazandók.

— GEN-6.3.3-02 A CP azonosítója [VÁLASZTHATÓ]:

a) [QCP-l]

— az 5.3. szakasz b) pontjában meghatározottak szerinti, és/vagy

— a TSP, más releváns érdekelt fél vagy más szabványosítási szervezet által az e dokumentumban meghatározott alkalmazandó követelményeket pontosító hitelesítési rendhez kiosztott objektumazonosító (OID);

b) [QCP-l-qscd]

— az 5.3. szakasz d) pontjában meghatározottak szerinti, és/vagy

— a TSP, más releváns érdekelt fél vagy más szabványosítási szervezet által az e dokumentumban meghatározott alkalmazandó követelményeket pontosító hitelesítési rendhez kiosztott objektumazonosító (OID).

7. 6.3.5. Kulcspár- és tanúsítványhasználat

— SDP-6.3.5-02A [FELTÉTELES] Ha a TSP kezeli az alany helyett a QSCD-t, a TSP olyan minősített bizalmi szolgáltató, amely a 910/2014/EU rendelettel [i.1] összhangban távoli minősített bélyegzőt létrehozó eszköz kezelésére irányuló minősített bizalmi szolgáltatást nyújt.

— SDP-6.3.5-11A Az előfizető kötelezettségei (lásd a 6.3.4. szakaszt), ha az előfizető vagy az alany létrehozza az alany kulcsait:

a) arra vonatkozó kötelezettség, hogy az alany kulcsait az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [7] megfelelő algoritmus használatával hozzák létre a tanúsított kulcsnak a CP-ben meghatározott felhasználási céljaira; valamint

b) arra vonatkozó kötelezettség, hogy az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [7] megfelelő kulcshosszt és algoritmust használjanak a tanúsítvány érvényességi ideje során a tanúsított kulcsnak a CP-ben meghatározott felhasználási céljaira.

8. 6.3.10. Tanúsítványstátusz-szolgáltatások

— CSS-6.3.10-08 [FELTÉTELES] Ha rendelkezésre áll tanúsítvány-visszavonási lista (CRL), a TSP gondoskodik arról, hogy legalább a CSS-6.3.10-12 pontban előírt tanúsítványalkalmazási nyilatkozatban (CPS) meghatározott ideig megmaradjon az utolsó CRL integritása és rendelkezésre állása.

9. 6.4.4. Személyzeti ellenőrzések

— OVR-6.4.4-02 A TSP bizalmi szerepet betöltő személyzete és adott esetben bizalmi szerepet betöltő alvállalkozói képesek teljesíteni a formális képzés és bizonyítványok, illetve a tényleges szakmai tapasztalat, vagy pedig a kettő kombinációja révén szerzett szaktudásra, tapasztalatra és képesítésre vonatkozó követelményt.

— OVR-6.4.4-03 Az OVR-6.4.4-02 követelmény betartása magában foglalja az új fenyegetésekre és a jelenlegi biztonsági gyakorlatokra vonatkozó rendszeres (legalább 12 havi) tájékoztatást.

— OVR-6.4.4-04 Az ETSI EN 319 401 szabványban [1] (7.2-15. szakasz) meghatározott bizalmi szerepek mellett a TS 419261 szabványban [6] meghatározott felelősségi körökkel rendelkező, nyilvántartásba vételért és visszavonásért felelős tisztviselők bizalmi szerepei is támogatandók. Azokban az esetekben, amikor a minősített bizalmi szolgáltatót (QTSP) egy tagállam vagy közigazgatási szerv közvetlenül irányítja, illetve az utóbbiak nevében más működteti, ezeket a további bizalmi szerepeket a helyi vagy regionális közigazgatásban feladatot ellátó, nyilvántartásba vételért és visszavonásért felelős tisztviselőket helyettesítő és azok nevében eljáró egy vagy több hivatalos képviselő is betöltheti.

10. 6.4.9. Tanúsító vagy nyilvántartó hatóság általi megszüntetés

— OVR-6.4.9-02 A TSP-nek a szolgáltatás megszüntetésére vonatkozó terve megfelel a 910/2014/EU rendelet [i.1] 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusokban meghatározott követelményeknek.

11. 6.5.1. Kulcspárok létrehozása és telepítése

— OVR-6.5.1-01A A tanúsító hatóság (CA) kulcspárjának generálását az európai kiberbiztonsági tanúsítási csoport által jóváhagyott, az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [7] a CA aláírási célja tekintetében megfelelő algoritmus alkalmazásával kell végezni.

— OVR-6.5.1-01B A CA aláírási kulcsához kiválasztott kulcshossz és algoritmus a CA aláírási célja tekintetében megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott, az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [7].

— OVR-6.5.1-01C [FELTÉTELES] Ha a CA generálja az alany kulcsait, a CA által létrehozott alanykulcsok a tanúsítvány érvényességi ideje alatt a CP-ben meghatározott célok tekintetében megfelelnek az európai kiberbiztonsági tanúsítási csoport által jóváhagyott, az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [7].

12. 6.5.2. A személyes kulcs védelme és a kriptográfiai modulok műszaki ellenőrzései

— GEN-6.5.2-01 Az ETSI EN 319 411-1 szabvány [2] 6.5.2. szakaszában meghatározott összes követelmény alkalmazandó, az OVR-6.5.2-01, OVR-6.5.2-03 és OVR-6.5.2-04 követelmények kivételével.

— GEN-6.5.2-02 A TSP kulcspárjának generálását – beleértve a visszavonási és nyilvántartásba vételi szolgáltatások által használt kulcsokét is – olyan biztonságos kriptográfiai eszközön belül kell végrehajtani, amely az alábbiaknak megfelelően tanúsított, megbízható rendszer:

  — az informatikai biztonságértékelés közös kritériumai az ISO/IEC 15408 szabvány [10] szerint vagy az informatikai biztonságértékelés közös kritériumainak megfelelően, CC:2002 verzió, 1–5. rész, közzétéve az informatikai biztonság területén a közös kritériumokra vonatkozó tanúsítványok elismeréséről szóló megállapodás résztvevői által, EAL 4 vagy magasabb szintű tanúsítással, vagy

  — a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) [8][9], EAL 4 vagy magasabb szintű tanúsítással, vagy

  — 2030.12.31-ig a FIPS PUB 140-3 szabvány [11] 3. szintje.

A tanúsítás kockázatelemzés alapján, fizikai és egyéb, nem technikai biztonsági intézkedések figyelembevételével történik, olyan biztonsági cél vagy védelmi profil, illetve modulterv- és biztonsági dokumentáció szerint, amely megfelel a jelen dokumentumban szereplő követelményeknek.

Ha a biztonságos kriptográfiai eszköz EUCC [8][9] tanúsítással rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják.

— GEN-6.5.2-03 A CA személyes aláírási kulcsát a GEN-6.5.2-01 és a GEN-6.5.2-02 pont követelményeinek megfelelő biztonságos kriptográfiai eszközön belül tárolják és használják.

13. 6.5.7. Hálózatbiztonsági ellenőrzések

— OVR-6.5.7-02 Az ETSI EN 319 401 szabvány [1] REQ-7.8-13 követelményében előírt sebezhetőségi vizsgálatot negyedévente legalább egyszer elvégzik.

— OVR-6.5.7-03 Az ETSI EN 319 401 szabvány [1] REQ-7.8-17X követelményében előírt behatolási tesztelést évente legalább egyszer elvégzik.

— OVR-6.5.7-04 A tűzfalakat úgy konfigurálják, hogy megakadályozzák a TSP működéséhez nem szükséges protokollok használatát és hozzáférést.

14. 6.6.1. Tanúsítványprofil

— GEN-6.6.1-05 A tanúsítvány tartalmazza a GEN-6.3.3-02 [VÁLASZTHATÓ] pontban meghatározott hitelesítésirend-azonosítók egyikét.

2. Az ETSI EN 319 412-3 esetében

1. 2.1. Normatív hivatkozások

— [2] ETSI EN 319 412-2 V2.4.1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons” (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványprofilok. 2. rész: Tanúsítványprofil a természetes személyek számára kibocsátott tanúsítványokhoz).

2. 4.2.1. Alany

— LEG-4.2.1-6 Az organizationIdentifier attribútum tartalmazza az alany szervezetnek a szervezet nevétől eltérő azonosítóját. Ha ismert megfelelő nyilvántartási szám, akkor az organizationIdentifier attribútum értéke a nyilvántartási számot megállapító hivatalos nyilvántartásban feltüntetett nyilvántartási számot tartalmazza.

3. Az ETSI EN 319 412-2 esetében:

1. 2.1. Normatív hivatkozások

— [2] ETSI EN 319 412-5 V2.5.1 „Electronic Signatures and Infrastructures (ESI). Certificate Profiles. Part 5: QCStatements” (Elektronikus aláírások és infrastruktúrák (ESI). Tanúsítványprofilok. 5. rész: QCStatements).

— [9] Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms” (Elfogadott kriptográfiai mechanizmusok), az ENISA kiadványa.

2. 2.2. Tájékoztató hivatkozások

— [i.7] érvénytelen.

3. 4.2.2. Aláírás

— GEN-4.2.2-2 Az aláírási algoritmus kiválasztása az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [9] összhangban történik.

— MEGJEGYZÉS érvénytelen.

4. 4.2.3.1. Jogi személynek minősülő kibocsátók

   — GEN-4.2.3.1-3 Ha ismert megfelelő nyilvántartási szám, akkor a kibocsátó azonosító adataiban szereplő organizationIdentifier értéke a nyilvántartási számot megállapító hivatalos nyilvántartásban feltüntetett nyilvántartási számot tartalmazza.

5. 4.2.5. Az alany nyilvános kulcsának adatai

   — GEN-4.2.5-2 Az alany nyilvános kulcsának kiválasztása az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [9] összhangban történik.

   — MEGJEGYZÉS érvénytelen.

6. 4.2.6. Sorozatszám

   — GEN-4.2.6-01 A tanúsítvány (IETF RFC 5280 szabvány [1] 4.1.2.2. szakaszában meghatározott) serialNumber értéke a TSP által kibocsátott minden egyes tanúsítvány esetében egyedi.