2025/1942

2025.9.30.

# A BIZOTTSÁG (EU) 2025/1942 VÉGREHAJTÁSI RENDELETE

**(2025. szeptember 29.)**

**a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített elektronikus aláírásokra irányuló minősített érvényesítési szolgáltatások és a minősített elektronikus bélyegzőkre irányuló minősített érvényesítési szolgáltatások 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 33. cikke (2) bekezdésére és 40. cikkére,

mivel:

(1) A minősített elektronikus aláírásokra és minősített elektronikus bélyegzőkre irányuló minősített érvényesítési szolgáltatások szavatolják az elektronikus aláírások, illetve elektronikus bélyegzők érvényesítési folyamatának és az érvényesítés eredményének integritását, hitelességét és helyességét. Az említett minősített bizalmi szolgáltatások kulcsszerepet töltenek be a digitális üzleti környezetben, elősegítve a hagyományos papíralapú eljárásokról az elektronikus megfelelőikre való átállást.

(2) A 910/2014/EU rendelet 33. cikkének (2) bekezdésében és 40. cikkében meghatározott megfelelési vélelem csak akkor alkalmazandó, ha a minősített elektronikus aláírásokra és minősített elektronikus bélyegzőkre irányuló minősített érvényesítési szolgáltatások megfelelnek az e rendeletben meghatározott technikai 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 további ellenőrzéseket foglaljanak magukban, amelyek garantálják a minősített bizalmi szolgáltatásoknak a biztonságát és megbízhatóságát, valamint a minősített elektronikus aláírások és a minősített elektronikus bélyegzők minősített státuszának és műszaki érvényességének ellenőrizhetőségét.

(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.

([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).

(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.

(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*

**Referenciaszabványok és specifikációk**

A 910/2014/EU rendelet 33. cikkének (2) bekezdésében és 40. cikkében említett referenciaszabványokat és specifikációkat e rendelet 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

([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).

([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).

*MELLÉKLET*

**A minősített elektronikus aláírásokra irányuló minősített érvényesítési szolgáltatások és a minősített elektronikus bélyegzőkre irányuló minősített érvényesítési szolgáltatásokra vonatkozó referenciaszabványok és specifikációk jegyzéke**

Az ETSI TS 119 441 V1.2.1 (2023-10) ([1]) (a továbbiakban: ETSI TS 119 441) és az ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) (a továbbiakban: ETSI TS 119 172-4) szabvány alkalmazandó, a következő kiigazításokkal:

1. Az ETSI TS 119 441 esetében

1. 2.1. Normatív hivatkozások

— [1] ETSI TS 119 101 V1.1.1 (2016-03) „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation" (Elektronikus aláírások és infrastruktúrák (ESI). Aláírás létrehozására és aláírás érvényesítésére szolgáló alkalmazásokra vonatkozó szabályzati rend és biztonsági követelmények).

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

— [3] ETSI EN 319 102-1 V1.4.1 (2024-06) „Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation" (Elektronikus aláírások és infrastruktúrák (ESI). Eljárások AdES digitális aláírások létrehozásához és érvényesítéséhez. 1. rész: Létrehozás és érvényesítés).

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

— [5] érvénytelen.

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

— [7] A Bizottság (EU) 2024/482 végrehajtási rendelete a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról ([3]).

— [8] ETSI TS 119 172-4 V1.1.1 (2021-05) „Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists" (Elektronikus aláírások és infrastruktúrák (ESI). Aláírási szabályzati rendek. 4. rész: Aláírás-alkalmazhatósági szabályok [érvényesítési szabályzati rend] a bizalmi listákat alkalmazó európai minősített elektronikus aláírásokhoz/bélyegzőkhöz).

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) „Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report" (Elektronikus aláírások és infrastruktúrák (ESI). Eljárások AdES digitális aláírások létrehozásához és érvényesítéséhez. 2. rész: Aláírás-érvényesítési jelentés).

— [10] Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms" (elfogadott kriptográfiai mechanizmusok), az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kiadványa ([4]).

— [11] A Bizottság (EU) 2024/3144 végrehajtási rendelete az (EU) 2024/4822 végrehajtási rendeletnek az alkalmazandó nemzetközi szabványok tekintetében történő módosításáról és az említett végrehajtási rendelet helyesbítéséről ([5]).

— [12] ETSI EN 319 411-1 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements" (Elektronikus aláírások és bizalmi infrastruktúrák (ESI). Tanúsítványokat kibocsátó bizalmi szolgáltatókra vonatkozó szabályzati rend és biztonsági követelmények. 1. rész: Általános követelmények).

([1]) ETSI TS 119 441 - „Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services" (Elektronikus aláírások és infrastruktúrák (ESI). Aláírás-érvényesítési szolgáltatásokat nyújtó bizalmi szolgáltatókra vonatkozó szabályzati rend követelményei), V1.2.1. (2023-10).

([2]) ETSI TS 119 172-4 - „Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists" (Elektronikus aláírások és infrastruktúrák (ESI). Aláírási szabályzati rendek. 4. rész: Aláírás-alkalmazhatósági szabályok [érvényesítési szabályzati rend] a bizalmi listákat alkalmazó európai minősített elektronikus aláírásokhoz/bélyegzőkhöz), V1.1.1 (2021-05).

([3]) HL L, 2024/482, 2024.2.7., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

([5]) HL L, 2024/3144, 2024.12.19., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2. 2.2. Tájékoztató hivatkozások

— [i.11] érvénytelen.

3. 3.3. Rövidítések

— EUCC: közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer.

4. 4.3.3. Folyamat

— 10. MEGJEGYZÉS Az uniós minősített aláírással vagy bélyegzővel kapcsolatos ügyekben iránymutatásért lásd az ETSI EN 319 102-1 szabványt [3], további iránymutatásért pedig az ETSI TS 119 172-4 szabványt [8].

5. 6.1. Az aláírás-érvényesítési szolgáltatásra vonatkozó alkalmazási nyilatkozat

— OVR-6.1-02 Az aláírás-érvényesítési szolgáltatásra (SVS) vonatkozó alkalmazási nyilatkozat struktúrája az A. mellékletnek felel meg.

— OVR-6.1-03 Az SVS szolgáltatásra vonatkozó alkalmazási nyilatkozatban fel kell sorolni a támogatott SVS-szabályzatokat, vagy hivatkozni kell rájuk (például objektumazonosítókkal, azaz OID-kkel), és röviden ismertetni kell őket.

6. 6.3. Információbiztonsági szabályzat

— OVR-6.3-02 A biztonsági szabályzat dokumentálja a személyes adatok védelme érdekében végrehajtott biztonsági és adatvédelmi ellenőrzéseket.

7. 7.2. Emberi erőforrások

— OVR-7.2-02 Az aláírás-érvényesítési szolgáltató (SVSP) 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-7.2-03 Az OVR-7.2-02 követelmény betartása magában foglalja az új fenyegetésekre és a jelenlegi biztonsági gyakorlatokra vonatkozó (legalább 12 havi) rendszeres tájékoztatást.

8. 7.5. Kriptográfiai ellenőrzések

— OVR-7.5-02 [FELTÉTELES] Az érvényesítési jelentések aláírásakor az SVSP személyes aláírási kulcsának megfelelő nyilvános aláírási SVSP-tanúsítványt megbízható tanúsító hatóság bocsátja ki, az ETSI EN 319 411-1 szabványban [12] meghatározott NCP+ hitelesítési renddel összhangban. A tanúsítványt az ETSI EN 319 411-2 szabványban [i.17] meghatározott megfelelő hitelesítési renddel összhangban kell kiállítani.

— OVR-7.5-03 [FELTÉTELES] Az érvényesítési jelentések aláírásakor az SVSP személyes aláírási kulcsát biztonságos kriptográfiai eszközön belül tárolják és használják, amely az alábbiaknak megfelelően tanúsított, megbízható rendszer:

a) az informatikai biztonságértékelés közös kritériumai az ISO/IEC 15408 szabvány [4] szerint vagy az informatikai biztonságértékelés közös kritériumainak megfelelően, CC:2022 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

b) az EUCC [7][11], EAL 4 vagy magasabb szintű tanúsítással; vagy

c) 2030.12.31-ig a FIPS PUB 140-3 szabvány [6] 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 [7][11] tanúsítással rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják.

— OVR-7.5-04 érvénytelen.

— OVR-7.5-06 Az SVSP személyes aláírási kulcsa csak akkor exportálható és importálható másik biztonságos kriptográfiai eszközbe, ha az exportálást és importálást biztonságosan és az említett eszközök tanúsításával összhangban hajtják végre.

9. 7.7. Üzembiztonság

— OVR-7.7-02 Annak biztosítása érdekében, hogy az alkalmazás fejlesztésére használt rendszerek megfelelő biztonsági intézkedéseket alkalmazzanak, és alkalmazkodjanak a konkrét alkalmazási környezetekhez, az aláírás-érvényesítési alkalmazásnak (SVA) olyan alkalmazási környezetet kell használnia, amelyet naprakész biztonsági javításokkal tartanak karban.

— OVR-7.7-03 Az ETSI TS 119 101 szabvány [1] 5.2. szakaszában meghatározott következő követelmények alkalmazandók az SVA-ra: GSM 1.3.

10. 7.8. Hálózatbiztonság

— OVR-7.8-02 Amennyiben megengedett a bizalmas adatokat tároló vagy kezelő rendszerekhez való távoli hozzáférés, hivatalos szabályzatot kell elfogadni, amelyet az OVR-6.3-02 követelményben előírt elemek részeként kell ismertetni.

— OVR-7.8-04 Az ETSI EN 319 401 szabvány [1] REQ-7.8-13 követelményében előírt sebezhetőségi vizsgálatot negyedévente legalább egyszer elvégzik.

— OVR-7.8-05 Az ETSI EN 319 401 szabvány [1] REQ-7.8-17X követelményében előírt behatolási tesztelést évente legalább egyszer elvégzik.

— OVR-7.8-06 A tűzfalakat úgy konfigurálják, hogy megakadályozzák az SVSP működéséhez nem szükséges protokollok használatát és hozzáférést.

11. 7.12. Az aláírás-érvényesítési szolgáltatás nyújtásának megszüntetése és megszüntetési tervei

— OVR-7.12-02 A bizalmi szolgáltatónak (TSP) a szolgáltatás megszüntetésére vonatkozó terve megfelel a 910/2014/EU rendelet [i.1] 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusokban meghatározott követelményeknek.

12. 7.14. Ellátási lánc

— OVR-7.14-01 Az ETSI EN 319 401 szabvány [2] 7.14. szakaszában meghatározott követelmények alkalmazandók.

13. 8.1. Aláírás-érvényesítési eljárás

— VPR-8.1-07 Az érvényesítési alkalmazás (SVA) megfelel az ETSI TS 119 101 szabvány [1] 7.4. szakasza SIA 1 – SIA 4 pontjában foglalt követelményeknek.

— VPR-8.1-11 [FELTÉTELES] Amennyiben az SVS a 910/2014/EU rendelet [i.1] 32. cikkének (1) bekezdésével (illetve 40. cikkével) összhangban minősített elektronikus aláírásokat vagy minősített elektronikus bélyegzőket kíván érvényesíteni, az érvényesítési folyamatnak az ETSI TS 119 172-4 szabvány [8] követelményeit kell követnie.

14. 8.2. Aláírás-érvényesítési protokoll

— SVP-8.2-03 Az aláírás-érvényesítési válaszon fel kell tüntetni az SVS-szabályzat OID-jét.

15. 8.4. Aláírás-érvényesítési jelentés

— SVR-8.4-02 Az érvényesítési jelentés megfelel az ETSI TS 119 102-2 szabványnak [9].

— SVR-8.4-07 [FELTÉTELES] Amennyiben az SVS nem dolgozta fel teljes mértékben az aláírás-érvényesítési szabályzatot, a jelentésnek az érvényesített korlátok mellett be kell számolnia a figyelmen kívül hagyott vagy felülbírált korlátokról is.

— SVR-8.4-15 Az érvényesítési jelentés egyértelműen feltünteti az egyes létezésigazolások eredetét (az aláíráson belülről, a kliensről, a szerverről).

— SVR-8.4-16 Az érvényesítési jelentésen szerepel az érvényesítési jelentés aláírása, amely az SVSP digitális aláírása.

— SVR-8.4-17 [FELTÉTELES] Az érvényesítési jelentések aláírásakor az aláírás formátuma és célja megfelel az ETSI TS 119 102-2 szabványnak [9].

16. 9. Az e dokumentumban meghatározott bizalmi szolgáltatási szabályzatra épülő érvényesítési szolgáltatási szabályzatok meghatározásának kerete:

— OVR-9-05 [FELTÉTELES] Amennyiben az SVS az e dokumentumban meghatározott bizalmi szolgáltatási szabályzatra épül, kockázatértékelést kell végezni az üzleti követelmények értékeléséhez, valamint a megadott közösség és az alkalmazhatóság érdekében a szabályzatba foglalandó biztonsági követelmények meghatározásához.

— OVR-9-06 [FELTÉTELES] Amennyiben az SVS-szabályzat az e dokumentumban meghatározott bizalmi szolgáltatási szabályzatra épül, egy meghatározott felülvizsgálati folyamatnak megfelelően kell jóváhagyni és módosítani a szabályzatot, kitérve a fenntartásával kapcsolatos felelősségi körökre is.

— OVR-9-07 [FELTÉTELES] Amennyiben az SVS-szabályzat az e dokumentumban meghatározott bizalmi szolgáltatási szabályzatra épül, egy meghatározott felülvizsgálati folyamatnak kell léteznie annak biztosítására, hogy a szabályzatot támogassák az alkalmazási nyilatkozatok.

— OVR-9-08 [FELTÉTELES] Amennyiben az SVS-szabályzat az e dokumentumban meghatározott bizalmi szolgáltatási szabályzatra épül, a TSP a felhasználói közössége rendelkezésére bocsátja a TSP által támogatott szabályzatokat.

— OVR-9-09 [FELTÉTELES] Amennyiben az SVS-szabályzat az e dokumentumban meghatározott bizalmi szolgáltatási szabályzatra épül, az előfizetők rendelkezésére kell bocsátani a TSP által támogatott szabályzatok módosításait.

17. B. melléklet (normatív) A 910/2014/EU rendelet 33. cikkében meghatározott, minősített elektronikus aláírást (QES) érvényesítő minősített érvényesítési szolgáltatás

— VPR-B-02 [FELTÉTELES] Ha az SVSP minősített aláírás-érvényesítési szolgáltató (QSVSP), a végrehajtás megfelel az ETSI TS 119 172-4 szabványnak [8].

— 2. MEGJEGYZÉS érvénytelen.

— OVR-B-04 [FELTÉTELES] Ha az SVSP QSVSP, az OVR-B-03 pontban említett tesztek különböző, pozitív és negatív felhasználási eseteket vizsgálnak.

— VPR-B-11 [FELTÉTELES] Ha az SVSP QSVSP, az SVSP ellenőrzi a hash számítást (vagy a szerveroldalon végzi a számítást, vagy a klienst ellenőrzi, ha az a kliensoldalon megengedett).

— 5. MEGJEGYZÉS érvénytelen.

— 6. MEGJEGYZÉS érvénytelen.

— VPR-B-15 [FELTÉTELES] Ha az SVSP QSVSP, a VPR-B-13 – VPR-B-14 követelmények kielégítése érdekében az érvényesítési jelentés megfelel az ETSI TS 119 102-2 szabványnak [9].

— VPR-B-16 [FELTÉTELES] Ha az SVSP QSVSP, a végrehajtás megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [10] a QES-t érvényesítő minősített érvényesítési szolgáltatások nyújtása során a megfelelő kriptográfiai technikák alkalmazása tekintetében.

18. C. melléklet (tájékoztató jellegű) A követelmények megfeleltetése a 910/2014/EU rendeletnek, az „Érvényesítés biztosítása a 32. cikk (1) bekezdésének megfelelően” című szakasz második bekezdése:

— A 910/2014/EU rendelet [i.1] 32. cikkének (1) bekezdésében és 40. cikkében előírt összes feltétel ellenőrzésének biztosítása érdekében helyes érvényesítési algoritmusra van szükség. Ez azonos determinisztikus eredményt ad az érvényesítésre benyújtott aláíráshoz vagy bélyegzőhöz. Ehhez kulcsfontosságú az aláírás-érvényesítési szabályzat. Az ETSI EN 319 102-1 [3] szabványban meghatározott érvényesítési algoritmuson alapuló ETSI TS 119 172-4 szabványt [8] ezt szem előtt tartva adták ki.

2. Az ETSI TS 119 172-4 esetében

1. 2.1. Normatív hivatkozások:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation” (Elektronikus aláírások és infrastruktúrák (ESI). Eljárások AdES digitális aláírások létrehozásához és érvényesítéséhez. 1. rész: Létrehozás és érvényesítés).

— Az „ETSI TS 119 102-1 [1]” szabványra való minden hivatkozást az „ETSI EN 319 102-1 [1]” szabványra való hivatkozásként kell értelmezni

— [2] ETSI TS 119 612 V2.3.1 (2024-11) „Electronic Signatures and Infrastructures (ESI); Trusted Lists” (Elektronikus aláírások és infrastruktúrák (ESI). Bizalmi listák).

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation” (Elektronikus aláírások és infrastruktúrák (ESI). Aláírás létrehozására és aláírás érvényesítésére szolgáló alkalmazásokra vonatkozó szabályzati rend és biztonsági követelmények).

2. 4.2. Érvényesítési korlátok és érvényesítési eljárások, REQ-4.2-03 követelmény, „X.509. Érvényesítési korlátok” szakasz, c) pont:

— i. Ha a végfelhasználói tanúsítvány bizalmi horgonyt jelent, a „RevocationCheckingConstraints” korlát nem használható.

— ii. Ha a végfelhasználói tanúsítvány nem jelent bizalmi horgonyt, a „RevocationCheckingConstraints” korlát értéke az ETSI TS 119 172-1 szabvány [3] A.4.2.1. szakasza A.2. táblázatának (m)2.1. sorában meghatározott „eitherCheck” beállítást kapja.

— iii. Ha a végfelhasználói tanúsítvány bizalmi horgonyt jelent, az ETSI TS 119 172-1 szabvány [3] A.4.2.1. szakasza A.2. táblázatának (m)2.2. sorában meghatározott „RevocationFreshnessConstraints” korlát nem használható.

— iv. Ha a végfelhasználói tanúsítvány nem jelent bizalmi horgonyt, az ETSI TS 119 172-1 szabvány [3] A.4.2.1. szakasza A.2. táblázatának (m)2.2. sorában meghatározott „RevocationFreshnessConstraints” korlát legfeljebb a 24 óra értéket veheti fel az aláírási tanúsítvány esetében. Az aláírási tanúsítványtól eltérő – többek között az időbélyegzőket támogató – tanúsítványok esetében nem határoznak meg értéket a „RevocationFreshnessConstraints” korlathoz.

3. 4.4. A műszaki alkalmazhatóság (szabályok) ellenőrzési folyamata

— REQ-4.4.2-03 Ha a REQ-4.4.2-01. pontban meghatározott ellenőrzések bármelyike sikertelen, akkor:

a) a folyamat leáll;

b) az aláírást technikailag meghatározatlanként kezelik, azaz nem minősül sem uniós minősített elektronikus aláírásnak, sem uniós minősített elektronikus bélyegzőnek;

c) a fenti eredmény és az összes közbenső eljárás folyamatainak eredményei tükröződnek az aláírás alkalmazhatósági szabályaira vonatkozó ellenőrzési jelentésben.