EURÓPAI
BIZOTTSÁG

Brüsszel, 2025.9.29.
C(2025) 6489 final

ANNEX

MELLÉKLET

a következőhöz:

A BIZOTTSÁG (EU) .../... VÉGREHAJTÁSI RENDELETE

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

MELLÉKLET

A 2. cikkben említett referenciaszabványok és specifikációk jegyzéke

Az ETSI TS 119 511 V1.1.1 (2019-06) (a továbbiakban: ETSI TS 119 511) és az ETSI TS 119 172-4 V1.1.1 (2021-05) (a továbbiakban: ETSI TS 119 172-4) szabvány alkalmazandó, a következő kiigazításokkal:

1. Az ETSI TS 119 511 esetében

1. 2.1. Normatív hivatkozások:

– [1] 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)

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

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

– [6] A Bizottság (EU) 2024/482 végrehajtási rendelete (2024. január 31.) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról[1]

– [7] A Bizottság (EU) 2024/3144 végrehajtási rendelete (2024. december 18.) az (EU) 2024/482 végrehajtási rendeletnek az alkalmazandó nemzetközi szabványok tekintetében történő módosításáról és az említett végrehajtási rendelet helyesbítéséről[2]

– [8] Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms” (Elfogadott kriptográfiai mechanizmusok), az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kiadványa[3]

– [9] 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)

– [10] ISO/IEC 15408:2022 (1–5. rész) „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security”

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

(Információbiztonság, kiberbiztonság és a magánélet védelme. Az informatikai biztonságértékelés kritériumai)

2. 3.1. Fogalommeghatározások

   – biztonságos kriptográfiai eszköz: a felhasználó személyes kulcsát tároló eszköz, amely megvédi az említett kulcsot a sérüléstől, és a felhasználó nevében aláírási vagy dekódolási funkciókat lát el

3. 6.4. Megőrzési profilok

   – OVR-6.4-08A [WTS][WOS] A bizonyíték várható időtartama megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [8]

   – 3. MEGJEGYZÉS érvénytelen

4. 6.5. A megőrzésre vonatkozó bizonyítékokkal kapcsolatos szabályzat

   – OVR-6.5-04A Az alkalmazott kriptográfiai algoritmusok megfelelnek az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [8]

   – 1. MEGJEGYZÉS érvénytelen

5. 7.2. Emberi erőforrások

   – OVR-7.2-02 A megőrzési szolgáltató (PSP) 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

6. 7.5. Kriptográfiai ellenőrzések

   – OVR-7.5-05 [FELTÉTELES] Amikor a PSP a megőrzésre vonatkozó bizonyítékot (vagy annak egy részét) aláírja, a PSP 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 [10] 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 [6][7], EAL 4 vagy magasabb szintű tanúsítással; vagy

     c) 2030.12.31-ig a FIPS PUB 140-3 szabvány [5] 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 [6][7] tanúsítással rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják

- OVR-7.5-06 [FELTÉTELES] érvénytelen
- OVR-7.5-07 [FELTÉTELES] Amikor a PSP a megőrzésre vonatkozó bizonyítékot (vagy annak egy részét) aláírja, a PSP személyes aláírási kulcsainak biztonsági másolatait biztonságos kriptográfiai eszközzel védik az integritásuk és bizalmas jellegük biztosítása érdekében, mielőtt az eszközön kívül tárolják őket
- OVR-7.5-08 A PSP 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

7. 7.8. Hálózatbiztonság
   - OVR-7.8-03 Az ETSI EN 319 401 szabvány [1] REQ-7.8-13 követelményében előírt sebezhetőségi vizsgálatot negyedévente legalább egyszer elvégzik
   - OVR-7.8-04 Az ETSI EN 319 401 szabvány [1] REQ-7.8-17X követelményében előírt behatolási tesztelést évente legalább egyszer elvégzik
   - OVR-7.8-05 A tűzfalakat úgy konfigurálják, hogy megakadályozzák a PSP működéséhez nem szükséges protokollok használatát és hozzáférést
8. 7.14. Kriptográfiai nyomon követés
   - OVR-7.14-03A Az OVR-7.14.01 és OVR-7.14.02 pontban említett kriptográfiai algoritmusok értékelése megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [8]
   - MEGJEGYZÉS érvénytelen
9. 7.12. A szolgáltatás bizalmi szolgáltató általi megszüntetése és a bizalmi szolgáltató szolgáltatásmegszüntetési tervei
   - OVR-7.12-01A A bizalmi szolgáltató (TSP) szolgáltatás megszüntetésére vonatkozó terve megfelel a 910/2014/EU rendelet [i.2] 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusokban meghatározott követelményeknek
10. 7.17. Ellátási lánc
    - OVR-7.17-01 Az ETSI EN 319 401 szabvány [1] 7.14. szakaszában meghatározott követelmények alkalmazandók
11. A. melléklet (normatív): A 910/2014/EU rendelet 34. cikkében meghatározott, minősített elektronikus aláírás megőrzésére vonatkozó minősített szolgáltatás
    - OVR-A-02 [PDS][PDS+PGD]

a) a megőrzési szolgáltatás megőriz az elektronikus aláírás vagy bélyegző minősített státuszának ellenőrzéséhez szükséges minden olyan információt, amely a megőrzési időszak végéig nem lenne nyilvánosan hozzáférhető;

b) a megőrzési szolgáltatás biztosítja, hogy a megőrzött információk a megőrzési időszak alatt bármely tetszőleges időpontban olyanok legyenek, hogy amennyiben azokat az ETSI TS 119 172-4 szabvány [9] 4.4. szakaszában meghatározott folyamat bemeneti adataként adják meg, e folyamat eredménye egyértelműen meghatározza, hogy a digitális aláírás vagy bélyegző a megőrzés időpontjában műszakilag alkalmas volt-e uniós minősített elektronikus aláírásként vagy uniós minősített elektronikus bélyegzőként való alkalmazásra

– OVR-A-03 [PDS][PDS+PGD] A megőrzésre vonatkozó bizonyítékban használt időbélyegzők a 910/2014/EU rendelet [i.2] szerinti minősített időbélyegzők

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) „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 [3] szabvány 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 0 értéket vehet fel az aláírási tanúsítvány esetében, ami biztosítja, hogy a visszavonási információt csak akkor fogadják el, ha azt a legjobb aláírási idő után bocsátották ki. Az aláírási tanúsítványtól eltérő – többek között az időbélyegzőket támogató – tanúsítványok esetében nem határoznak meg értéket a „RevocationFreshnessConstraints” korláthoz

3. 4.3. Az aláírás-érvényesítési és -alkalmazhatósági szabályok ellenőrzési gyakorlataira vonatkozó követelmények

– REQ-4.3-02 Az aláírás-érvényesítési alkalmazások megfelelnek az ETSI TS 119 101 [13] szabványnak

4. 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 folyamat leáll

  – az aláírást technikailag meghatározatlanként kezelik, azaz nem minősül sem uniós minősített elektronikus aláírásnak, sem uniós minősített elektronikus bélyegzőnek

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