2026/1735

2026.7.22.

A BIZOTTSÁG (EU) 2026/1735 VÉGREHAJTÁSI RENDELETE

(2026. július 15.)

az (EU) 2025/1569 végrehajtási rendeletnek az alkalmazandó szabványok és specifikációk tekintetében történő módosításáról

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 45d. cikke (5) bekezdésére, 45e. cikke (2) bekezdésére, 45f. cikke (6) bekezdésére és 45f. cikke (7) bekezdésére,

mivel:

(1) Az európai digitális személyiadat-tárcák fejlesztése terén a tagállamok közötti lehető legmagasabb szintű harmonizáció biztosítása érdekében a tárcákra vonatkozó technikai specifikációk az (EU) 2021/946 bizottsági ajánlás ([2]) alapján végzett munkára – különösen az architektúrára és a referenciakeretre – támaszkodnak. Mivel az architektúra és a referenciakeret jelentősen átalakult az (EU) 2025/1569 bizottsági végrehajtási rendelet ([3]) elfogadása óta, az (EU) 2025/1569 végrehajtási rendeletet most ennek megfelelően módosítani kell azért, hogy összhangba kerüljön az új szabványokkal és specifikációkkal.

(2) A 910/2014/EU rendelet célkitűzéseivel összhangban a Bizottság kiválasztotta, mely szabványok vonatkoznak az elektronikus attribútumtanúsítványok kibocsátására, kezelésére és ellenőrzésére alkalmazandó követelmények teljesítésére. E szabványoknak tükrözniük kell a bevett gyakorlatokat, és széles körben elismertnek kell lenniük az érintett ágazatokban. Szükség esetén ezeket a szabványokat ki kell igazítani vagy ki kell egészíteni annak érdekében, hogy biztosítsák az elektronikus attribútumtanúsítványok magas szintű biztonságát és integritását, ugyanakkor elősegítve a határokon átnyúló interoperabilitást és a belső piac hatékony működését. E célkitűzéssel összhangban ez a rendelet aktualizálja a minősített elektronikus attribútumtanúsítványok és a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok kibocsátására és érvénytelenítésére alkalmazandó követelményeket, és bevezeti a hiteles források alapján végzett ellenőrzések eredményeinek aláírására és bélyegzővel való ellátására vonatkozó követelményeket.

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

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

([2]) A Bizottság (EU) 2021/946 ajánlása (2021. június 3.) az európai digitális személyazonossági keretre irányuló összehangolt megközelítés közös uniós eszköztáráról (HL L 210., 2021.6.14., 51. o., ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) A Bizottság (EU) 2025/1569 végrehajtási rendelete (2025. július 29.) a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített elektronikus attribútumtanúsítványok és a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok tekintetében történő alkalmazására vonatkozó szabályok megállapításáról (HL L, 2025/1569, 2025.7.30., ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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).

([5]) 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).

(4) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([6]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2026. április 17-én véleményt ([7]) nyilvánított.

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

ELFOGADTA EZT A RENDELETET:

1. cikk

Az (EU) 2025/1569 végrehajtási rendelet módosításai

Az (EU) 2025/1569 végrehajtási rendelet a következőképpen módosul:

1. A 3. cikk (2) bekezdésének helyébe a következő szöveg lép:

„(2) Amennyiben a minősített elektronikus attribútumtanúsítványok szolgáltatói, illetve a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok szolgáltatói olyan elektronikus attribútumtanúsítványokat bocsátanak ki, amelyek az attribútumtanúsítási rendszerek katalógusában felsorolt rendszerek egyikéhez tartoznak, azoknak meg kell felelniük a megfelelő attribútumtanúsítási rendszer követelményeinek. A tanúsítványok kibocsátói által az attribútumtanúsítási rendszerek követelményeinek való megfelelés céljából kialakított szabályzatoknak és eljárásoknak a 910/2014/EU rendeletben meghatározott megfelelőségértékelés részét kell képezniük.”

2. A 4. cikk a következőképpen módosul:

a) az (1) bekezdést el kell hagyni;

b) a (3) bekezdés helyébe a következő szöveg lép:

„(3) A minősített elektronikus attribútumtanúsítványok szolgáltatói és a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok szolgáltatói, amennyiben a tanúsítványokat 24 óránál hosszabb érvényességi idővel állítják ki, legalább a következő körülmények fennállása esetén érvénytelenítik azokat:

a) azon személy kérésére, akinek a részére az elektronikus attribútumtanúsítványt kiállították, vagy adott esetben a tanúsítvány alanyának kérésére;

b) ha a szolgáltató tudomást szerez arról, hogy a minősített elektronikus attribútumtanúsítvány vagy a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítvány biztonsága vagy megbízhatósága veszélybe került;

c) az uniós vagy a nemzeti jog által megállapított egyéb helyzetekben.”

c) a (4) bekezdés helyébe a következő szöveg lép:

„(4) A minősített elektronikus attribútumtanúsítványok szolgáltatóinak és a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok szolgáltatóinak olyan érvénytelenítési technikákat és kezelési módszereket kell kialakítaniuk, amelyek tiszteletben tartják a magánéletet és kizárják az összekapcsolhatóságot és a nyomonkövethetőséget. Az érvénytelenítési technikáknak meg kell felelniük a II. mellékletben meghatározott követelményeknek.”

([6]) 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).

([7]) Az európai adatvédelmi biztos hivatalos észrevételei az adattárca-igénybevevők nyilvántartásba vételére alkalmazandó szabványok és specifikációkról szóló bizottsági végrehajtási rendelet tervezetéről |európai adatvédelmi biztos.

3. A 9. cikk a következőképpen módosul:

a) a szöveg a (2) bekezdés után a következő (2a) bekezdéssel egészül ki:

„(2a) Az ellenőrzési mechanizmusnak meg kell felelnie a IV. mellékletben meghatározott specifikációknak.”;

b) a (4) bekezdés helyébe a következő szöveg lép:

„(4) Az ellenőrzési eredmény azt tartalmazza, hogy az attribútum ellenőrzésére sor került-e, vagy sem, valamint a hiteles forrásért felelős közigazgatási szerv vagy adott esetben azon közigazgatási szerv megjelölését, amely az attribútum ellenőrzésére szolgáló hiteles forrás nevében eljár.

Az ellenőrzés eredményét a hiteles forrásért felelős közigazgatási szervnek vagy a nemzeti szinten elismert kijelölt köztes szereplőnek kell legalább az elektronikus aláírások minősített tanúsítványán alapuló, fokozott biztonságú elektronikus aláírással aláírnia, illetve az elektronikus bélyegzők minősített tanúsítványán alapuló, fokozott biztonságú elektronikus bélyegzővel ellátnia.”

4. Az I. melléklet helyébe e rendelet I. mellékletének szövege lép.

5. A II. melléklet helyébe e rendelet II. mellékletének szövege lép.

6. Az e rendelet III. mellékletében foglalt szöveg IV. mellékletként kerül beillesztésre.

2. cikk

Hatálybalépés

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

Az 1. cikk (3) bekezdése 2027. január 1-től alkalmazandó.

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

Kelt Brüsszelben, 2026. július 15-én.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

I. MELLÉKLET

„I. MELLÉKLET

A 3. cikkben említett referenciaszabványok és specifikációk jegyzéke

Az ETSI TS 119 471 V1.1.1 (2025-05) szabvány alkalmazandó, a következő kiigazításokkal:

1. 2.1. Normative references (Normatív hivatkozások):

   [1] ETSI EN 319 401 V3.2.1 (2026-01): „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] Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms" (Elfogadott kriptográfiai mechanizmusok), az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kiadványa;

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

   [4] A Bizottság (EU) 2024/482 végrehajtási rendelete ([1]);

   [5] A Bizottság (EU) 2024/3144 végrehajtási rendelete ([2]);

   [6] 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).

2. 3.1. Terms (Fogalommeghatározások):

   A szöveg a következő meghatározással egészül ki:

   — 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. 4. EAA trust services (Elektronikus attribútumtanúsítványokkal kapcsolatos bizalmi szolgáltatások)

   — A 4.2.2.2. pont – Verification of attributes against authentic sources („Attribútumellenőrzés hiteles források segítségével") – nem alkalmazandó.

   — REQ-EAASP-4.2.2.3-02: Az elektronikus attribútumtanúsítványt biztosító bizalmi szolgáltató (EAASP) érvényes hozzáférési tanúsítványt használó kölcsönös hitelesítési mechanizmusok révén hitelesíti az európai digitális személyiadat-tárca (EUDIW) példányt.

   — REQ-EAASP-4.2.2.3-03: Az EAASP érvényesíti az EUDIW-egységet, valamint azt, hogy *az EUDIW-példány visszavonásra került-e*.

   — A *4.3.2. pont –„EUDIW Specific*" (EUDIW-specifikus előírások) *–nem alkalmazandó*.

4. 6.1 EAAS practice statement (Az elektronikus attribútumtanúsítványokkal kapcsolatos szolgáltatásra [EAAS] vonatkozó alkalmazási nyilatkozat):

   — REQ-EAASP-6.1-02: Az EAASP az EAAS szolgáltatásra vonatkozó alkalmazási nyilatkozatban dokumentálja az érvénytelenítési mechanizmust.

5. 6.3. Information security policy (Információbiztonsági szabályzat):

   — REQ-EAASP-6.3-02: Az EAASP eljárásokat dolgoz ki arra vonatkozóan, hogy az üzleti követelményekkel és a vonatkozó jogszabályokkal és egyéb rendelkezésekkel, többek között a 910/2014/EU rendelet 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusok követelményeivel összhangban értesíti a felügyeleti szervet az elektronikus attribútumtanúsítványokkal kapcsolatos bizalmi szolgáltatás nyújtásában bekövetkezett bármely változásról és az e tevékenység megszüntetésére irányuló szándékról. Az EAASP a következők szerint értesíti a felügyeleti szervet:

     — legalább egy hónappal a változtatások végrehajtása előtt

     — legalább három hónappal a bizalmi szolgáltatás nyújtásának tervezett megszüntetése előtt.

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

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

6. 7.5. Cryptographic controls (Kriptográfiai ellenőrzések):

— REQ-EAASP-7.5.2-05: érvénytelen

— REQ-EAASP-7.5.2-06: érvénytelen

— REQ-EAASP-7.5.3-01A: Megfelelő biztonsági ellenőrzéseket kell alkalmazni a kriptográfiai kulcsoknak, a kriptográfiai algoritmusoknak és a kriptográfiai eszközöknek a teljes életciklusuk során történő kezelésére, adott esetben kriptográfiai agilitási megközelítést követve

— REQ-EAASP-7.5.3-01B: Bizalmi szolgáltatásainak nyújtása céljára az EAASP az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [2] kompatibilis, megfelelő kriptográfiai technikákat választ és alkalmaz

— REQ-EAASP-7.5.3-02: Az EAASP biztosítja, hogy az EAA digitális aláírásához vagy bélyegzőjéhez általa használt biztonságos kriptográfiai eszköz minősített aláírást vagy bélyegzőt létrehozó eszköz legyen, és hogy az elektronikus attribútumtanúsítványokkal kapcsolatos megfelelő bizalmi szolgáltatás – vagy annak egy része – nyújtásához használt minden egyéb digitális aláírást vagy bélyegzőt olyan biztonságos kriptográfiai eszközzel hozzanak létre, amely az alábbi lehetőségek egyikének megfelelően tanúsított, megbízható rendszer:

a) az informatikai biztonságértékelés közös kritériumai az informatikai biztonságértékelés közös kritériumai 3.1 (CC3.1) verziójának megfelelően (2027. augusztus 31-ig), vagy CC:2022 verziója, 1–5. részének megfelelően (közzétéve az informatikai biztonság területén a közös kritériumokra vonatkozó tanúsítványok elismeréséről szóló megállapodás résztvevői által), vagy az ISO/IEC 15408 [6] szabvány szerint, EAL 4 vagy magasabb szintű tanúsítással; vagy

b) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) [4][5], EAL 4 vagy magasabb szintű tanúsítással; vagy

c) a meglévő tanúsított rendszerek esetében a FIPS-140–2 3. szintje alkalmazandó 2027. augusztus 31-ig vagy a FIPS PUB 140–3 [3] 3. szintje 2030. december 31-ig.

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 [4][5] tanúsítással rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják

— REQ-EAASP-7.5.5-01: érvénytelen

— REQ-EAASP-7.5.5-02: érvénytelen

— REQ-EAASP-7.5.5-04: érvénytelen.

7. 7.9 Vulnerabilities and Incident management (Sebezhetőségek és incidenskezelés):

— REQ-EAASP-7.9-02: A nyomonkövetési tevékenységek során figyelembe veszik az összegyűjtött vagy elemzett információk érzékenységét.

8. 7.12. EAASP and EAAS termination and termination plans (Az EAASP és az EAAS megszüntetése és a megszüntetési tervek):

— REQ-EAASP-7.12-04: Az EAASP szolgáltatás megszüntetésére vonatkozó terve megfelel a 910/2014/EU rendelet [i.1] 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusokban meghatározott követelményeknek.”

II. MELLÉKLET

„II. MELLÉKLET

A 3. és 4. cikkben említett technikai specifikációk

A minősített elektronikus attribútumtanúsítványok és a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok szolgáltatói a tanúsítványokat az (EU) 2024/2979 bizottsági végrehajtási rendelet ([1]) II. mellékletében meghatározott legalább egy szabványnak megfelelően bocsátják ki, és a szintén az (EU) 2024/2979 bizottsági végrehajtási rendelet II. mellékletében meghatározott, releváns érvénytelenítési technikákat alkalmazzák.”

([1]) A Bizottság (EU) 2024/2979 végrehajtási rendelete (2024. november 28.) a 910/2014/EU európai parlamenti és tanácsi rendeletnek az európai digitális személyiadat-tárcák integritása és alapvető funkciói tekintetében történő alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/2979, 2024.12.4., ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

III. MELLÉKLET

„IV. MELLÉKLET

A 9. cikkben említett szabványok és technikai specifikációk jegyzéke

A 9. cikkben említett ellenőrzési mechanizmusoknak meg kell felelniük a következő specifikációk egyikének vagy mindkettőnek, az alábbi kiigazításokkal:

a) az ETSI TS 119 478 V1.1.1 (2026–01) - Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources (Elektronikus aláírások és bizalmi infrastruktúrák [ESI]; Hiteles forrásokhoz kapcsolódó interfészek specifikációi) szabvány 6.1.1. szakaszában meghatározott technikai specifikációk;

— REQ-ASIP-6.1.1.2-04-01 [FELTÉTELES]: Amennyiben az attributeVerificationResult értéke vagy http://uri.etsi.org/19478/VerificationResult/Match, vagy http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, az attributeVerificationResult tartalmazhat attributeValue elemet

— REQ-ASIP-6.1.1.2-04-02 [FELTÉTELES]: Amennyiben a kapott attributeVerificationResult érték http://uri.etsi.org/19478/VerificationResult/Match, és az attributeVerificationResult attribútum tartalmaz attributeValue elemet, az attributeValue elemnek a kérelemben szereplő értéket kell tartalmaznia.

— REQ-ASIP-6.1.1.2-04-03 [FELTÉTELES]: Amennyiben a kapott attributeVerificationResult érték http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, és az attributeVerificationResult attribútum tartalmaz attributeValue elemet, az attributeValue elemnek a hiteles forrásban tárolt attribútumértéket kell tartalmaznia.

— REQ-ASIP-6.1.1.2-06-04-01 [FELTÉTELES]: Amennyiben a fragmentVerificationResult értéke vagy http://uri.etsi.org/19478/VerificationResult/Match, vagy http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, az attributeVerificationResult tartalmazhat fragmentValue elemet;

— REQ-ASIP-6.1.1.2-06-04-02 [FELTÉTELES]: Amennyiben a kapott fragmentVerificationResult érték http://uri.etsi.org/19478/VerificationResult/Match, és az attributeVerificationResult attribútum tartalmaz fragmentValue elemet, a fragmentValue elemnek a kérelemben szereplő értéket kell tartalmaznia.

— REQ-ASIP-6.1.1.2-06-04-03 [FELTÉTELES]: Amennyiben a kapott fragmentVerificationResult érték http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, és az attributeVerificationResult attribútum tartalmaz fragmentValue elemet, a fragmentValue elemnek a hiteles forrásban tárolt attribútumértéket kell tartalmaznia.

b) az ETSI TS 119 478 V1.1.1 (2026–01) - Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources (Elektronikus aláírások és bizalmi infrastruktúrák [ESI]; Hiteles forrásokhoz kapcsolódó interfészek specifikációi) szabvány 6.2.3. szakaszában meghatározott technikai specifikációk;

— REQ-ASIP-6.2.3.2.1-08-04: Az AttributeVerificationResponse elem pontosan egy alárendelt elemet tartalmazhat, amely TextValue, XMLValue vagy AttributeProperties lehet.”