2025/1929

2025.9.30.

A BIZOTTSÁG (EU) 2025/1929 VÉGREHAJTÁSI RENDELETE

(2025. szeptember 29.)

a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített elektronikus időbélyegzők kibocsátása kapcsán a dátum és időpont adatokhoz való hozzárendelése és az időforrások pontosságának meghatározása 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 42. cikke (2) bekezdésére,

mivel:

(1) A minősített elektronikus időbélyegzők kulcsszerepet töltenek be a digitális üzleti környezetben, elősegítve a hagyományos papíralapú eljárásokról az elektronikus megfelelőikre való átállást. A minősített elektronikus időbélyegzők a dátum- és időpont-információknak az elektronikus adatokhoz való hozzárendelése révén segítenek szavatolni az általuk jelzett dátum és időpont pontosságát, valamint azon digitális dokumentumok integritását, amelyekhez hozzárendelték a dátumot és az időpontot.

(2) A 910/2014/EU rendelet 42. cikkének (1a) bekezdésében meghatározott megfelelési vélelem csak akkor alkalmazandó, ha a minősített időbélyegzők 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 további ellenőrzéseket foglaljanak magukban amelyek garantálják a minősített bizalmi szolgáltatásnak, valamint a dátum és időpont adatokhoz való hozzárendelésének és az időforrás pontosságának a biztonságát és megbízhatóságát.

(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 végrehajtási 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

A 910/2014/EU rendelet 42. cikkének (2) bekezdésében említett referenciaszabványokat és specifikációkat e rendelet melléklete tartalmazza.

2. cikk

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).

MELLÉKLET

A minősített időbélyegző-szolgáltatásokra vonatkozó referenciaszabványok és specifikációk jegyzéke

Az ETSI EN 319 421 V1.3.1 ([1]) (a továbbiakban: ETSI EN 319 421) és az ETSI EN 319 422 V1.1.1 ([2]) (a továbbiakban: ETSI EN 319 422) szabvány alkalmazandó, a következő kiigazításokkal:

1. Az ETSI EN 319 421 esetében

1. 2.1. Normatív hivatkozások:

— [3] 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).

— [4] 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).

— [5] ETSI EN 319 422 V1.1.1 (2016-03): „Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles" (Elektronikus aláírások és infrastruktúrák (ESI). Időbélyegző protokoll és időbélyegjelkép-profilok).

— [6] érvénytelen.

— [9] Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms" (Elfogadott kriptográfiai mechanizmusok), az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kiadványa ([3]).

— [10] 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 ([4]).

— [11] 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 ([5]).

2. 3.1. Fogalommeghatározások

— tanúsítvány érvényességi ideje: az a „notBefore" értéktől a „notAfter" értékig (az utóbbit is beleértve) tartó időintervallum, amelynek folyamán a tanúsító hatóság garantálja, hogy megőrzi a tanúsítvány státuszára vonatkozó információkat.

3. 3.3. Rövidítések

— EUCC: közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer.

4. 6.2. A bizalmi szolgáltatásra vonatkozó alkalmazási nyilatkozat

— OVR-6.2-03 Az időbélyegzés-szolgáltató (TSA) a TSA-közzétételi nyilatkozatban nyilatkozik az időbélyegzés szolgáltatásának rendelkezésre állásáról.

5. 7.3. Személyzeti biztonság

— OVR-7.3-02 A TSA 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-7.3-03 Az OVR-7.3-02 követelmény betartása magában foglalja az új fenyegetésekre és a jelenlegi biztonsági gyakorlatokra vonatkozó (legalább 12 havi) rendszeres tájékoztatást.

([1]) EN 319 421 – Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time Stamps, V1.3.1. (Elektronikus aláírások és infrastruktúrák (ESI). Időbélyegeket kibocsátó bizalmi szolgáltatókra vonatkozó szabályzati rend és biztonsági követelmények).

([2]) EN 319 422 – Electronic Signatures and Infrastructures (ESI) - Time-stamping protocol and time-stamp token profiles, V1.1.1 (2016-03) (Elektronikus aláírások és infrastruktúrák (ESI). Időbélyegző protokoll és időbélyegjelkép-profilok), https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.

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

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

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

6. 7.6.2. Az időbélyegző egység kulcsának generálása

— TIS-7.6.2-03 Az időbélyegző egység (TSU) kulcsának (kulcsainak) generálását olyan biztonságos kriptográfiai eszközön belül kell végrehajtani, amely az alábbiaknak megfelelően tanúsított, megbízható rendszer:

a) az informatikai biztonságértékelés közös kritériumai az ISO/IEC 15408 szabvány [3] 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 [10][11], EAL 4 vagy magasabb szintű tanúsítással; vagy

c) 2030.12.31.-ig a FIPS PUB 140-3 szabvány [7] 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 [10][11] tanúsítással rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják.

— TIS-7.6.2-04 érvénytelen.

— 3. MEGJEGYZÉS érvénytelen.

— TIS-7.6.2-05A A TSU kulcsgenerálási algoritmusa, az ezzel létrehozott aláírási kulcshossz és az aláírási algoritmus, amelyet az időbélyegzőknek, illetve a TSU nyilvánoskulcs-tanúsítványainak aláírásához használnak, megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [9].

— 4. MEGJEGYZÉS érvénytelen.

— TIS-7.6.2-06 A TSU 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. 7.6.3. Az időbélyegző egység személyes kulcsának védelme

— TIS-7.6.3-02 A TSU személyes 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 [3] 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

b) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) [10][11], EAL 4 vagy magasabb szintű tanúsítással; vagy

c) 2030.12.31.-ig a FIPS PUB 140-3 szabvány [7] 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 [10][11] tanúsítással rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják.

— TIS-7.6.3-03 érvénytelen.

— 2. MEGJEGYZÉS érvénytelen.

8. 7.6.7. A TSU-kulcs életciklusának vége

— TIS-7.6.7-03A A TSU személyes kulcsainak lejárati időpontja megfelel az elfogadott kriptográfiai mechanizmusoknak [9].

— 1. MEGJEGYZÉS érvénytelen.

9. 7.10. Hálózatbiztonság

— OVR-7.10-05 Az ETSI EN 319 401 szabvány [1] REQ-7.8-13 követelményében előírt sebezhetőségi vizsgálatot negyedévente legalább egyszer elvégzik.

— OVR-7.10-06 Az ETSI EN 319 401 szabvány [1] REQ-7.8-17X követelményében előírt behatolási tesztelést évente legalább egyszer elvégzik.

— OVR-7.10-07 A tűzfalakat úgy konfigurálják, hogy megakadályozzák a TSA működéséhez nem szükséges protokollok használatát és hozzáférést.

10. 7.14. A szolgáltatás TSA általi megszüntetése és a szolgáltató szolgáltatásmegszüntetési tervei

— OVR-7.14-01A A bizalmi szolgáltató (TSP) szolgáltatás megszüntetésére vonatkozó terve megfelel a 910/2014/EU rendelet [i.4] 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusokban meghatározott követelményeknek.

2. Az ETSI EN 319 422 esetében

1. 2.1. Normatív hivatkozások

— [5] érvénytelen.

— [6] érvénytelen.

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

— [9] RFC 9110 HTTP Semantics (HTTP-szemantika).

2. 4.1.3. A használandó hasító algoritmusok

— A következő szakasz alkalmazandó:

Az időbélyegzővel ellátandó információk hasításához használt hasító algoritmusok, az időbélyegző és a kiválasztott hasítófüggvények használhatóságának várható időtartama megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [8].

— MEGJEGYZÉS érvénytelen.

3. 4.2.3. A támogatandó algoritmusok

— A következő szakasz alkalmazandó:

A támogatandó időbélyegzőtoken-aláírási algoritmusok megfelelnek az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [8].

— MEGJEGYZÉS érvénytelen.

4. 4.2.4. A támogatandó kulcshosszok

— A következő szakasz alkalmazandó:

A kiválasztott aláírási algoritmushoz tartozó aláírásialgoritmus-kulcshosszok megfelelnek az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak.

— MEGJEGYZÉS érvénytelen.

5. 5.1.3. A támogatandó algoritmusok

— A következő szakasz alkalmazandó:

A támogatandó időbélyegző-adatokra vonatkozó hasító algoritmusok, valamint az időbélyegző és a kiválasztott hasítófüggvények használhatóságának várható időtartama megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [8].

— MEGJEGYZÉS érvénytelen.

6. 5.2.3. A használandó algoritmusok

— A következő szakasz alkalmazandó:

Az időbélyegzővel ellátandó információk hasításához használt hasító algoritmusok és az időbélyegzőtoken-aláírási algoritmusok megfelelnek az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [8].

— MEGJEGYZÉS érvénytelen.

7. 6.3. A kulcshosszra vonatkozó követelmények

— A következő szakasz alkalmazandó:

A TSU tanúsítványához kiválasztott aláírási algoritmus kulcshossza megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [8].

— MEGJEGYZÉS érvénytelen.

8. 6.5. Az algoritmusokra vonatkozó követelmények

— A következő szakasz alkalmazandó:

A TSU nyilvános kulcsa és a TSU tanúsítványának aláírása az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [8] összhangban alkalmaz algoritmusokat.

— MEGJEGYZÉS érvénytelen.

9. 7. A támogatandó szállítási protokollokhoz tartozó profilok

— Az időbélyegző kliens és az időbélyegző szerver az IETF RFC 3161 szabvány [1] 3.4. szakaszában meghatározottak szerint támogatja a HTTPS protokollal alkalmazott időbélyegző protokollt [9].

10. 8. A kriptográfiai algoritmusok objektumazonosítói

— A következő szakasz alkalmazandó:

A TSU nyilvános kulcsa és a TSU tanúsítványának aláírása az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [8] összhangban alkalmaz algoritmusokat.

11. 9.1. A rendeletnek való megfelelésre vonatkozó nyilatkozat

— Ha a TSA az időbélyegző-tokent a 910/2014/EU rendelet [i.2] szerinti minősített elektronikus időbélyegzőnek nyilvánítja, az az IETF RFC 3739 szabvány [i.3] 3.2.6. szakaszában meghatározott szintaxissal tartalmazza a qcStatements kiterjesztés egy példányát az időbélyegző-token kiterjesztés mezőjében.

— A qcStatements kiterjesztés tartalmazza a B. mellékletben meghatározott „esi4-qtstStatement-1” állítás egy példányát.

— A qcStatements kiterjesztés nem jelölhető meg kritikusként.