2025/2531

2025.12.17.

A BIZOTTSÁG (EU) 2025/2531 VÉGREHAJTÁSI RENDELETE

(2025. december 16.)

a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített elektronikus főkönyvekre vonatkozó referenciaszabványok és specifikációk 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 45 l. cikke (3) bekezdésére,

mivel:

(1) Az (EU) 2024/1183 európai parlamenti és tanácsi rendelet ([2]) kiegészítette a 910/2014/EU rendeletet az új bizalmi szolgáltatások és a minősített bizalmi szolgáltatások – köztük az elektronikus adatok minősített elektronikus főkönyvbe történő rögzítésére irányuló szolgáltatások – jegyzékével. A Bizottságnak össze kell állítania a szóban forgó szolgáltatásokra vonatkozó referenciaszabványok jegyzékét, és szükség esetén meg kell állapítania az említett szolgáltatásokra vonatkozó specifikációkat.

(2) Az elektronikus főkönyv elektronikus adatrekordok olyan sorozata, amely biztosítani hivatott ezen adatrekordok integritását és ezen adatrekordok időrendi sorrendjének pontosságát. Annak biztosítása érdekében, hogy az adatok minősített elektronikus főkönyvbe történő rögzítése időrend szerinti, következetes és megbízható legyen, közös specifikációkat kell megállapítani az elektronikus adatok minősített elektronikus főkönyvbe történő rögzítésére vonatkozóan.

(3) A 910/2014/EU rendelet 45 l. cikkének (2) bekezdésében meghatározott megfelelési vélelem csak akkor alkalmazandó, ha az elektronikus adatok minősített elektronikus főkönyvbe történő rögzítésére irányuló 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 azok további ellenőrzésekre is kiterjedjenek, amelyek garantálják a minősített bizalmi szolgáltatás biztonságát és megbízhatóságát.

(4) 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 státusának megadása vagy megerősítése során. A minősített bizalmi szolgáltatók azonban továbbra is alkalmazhatnak más gyakorlatot a 910/2014/EU rendelet követelményeinek való megfelelés igazolásához.

(5) A Bizottság rendszeresen értékeli az új technológiákat, gyakorlatokat, szabványokat és technikai specifikációkat. Az (EU) 2024/1183 rendelet (75) preambulumbekezdése értelmében a Bizottságnak rendszeresen felül kell vizsgálnia, és szükség esetén aktualizálnia kell ezt a rendeletet, hogy az folyamatosan megfeleljen a globális fejleményeknek, valamint az új technológiáknak, gyakorlatoknak, szabványoknak és 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).

(6) Az e rendelet szerinti személyesadat-kezelési tevékenységekre az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([3]) és adott esetben a 2002/58/EK európai parlamenti és tanácsi irányelv ([4]) alkalmazandó, figyelembe véve az Európai Adatvédelmi Testületnek a személyes adatok blokklánc-technológiákon keresztül történő kezeléséről szóló 02/2025. sz. iránymutatását ([5]) is.

(7) 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 2025. október 21-én véleményt nyilvánított ([7]).

(8) 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

E rendelet melléklete felsorolja a 910/2014/EU rendelet 45 l. cikkének (3) bekezdésében említett, a minősített elektronikus főkönyvekre vonatkozó referenciaszabványokat és specifikációkat.

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. december 16-án.

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]) edpb_guidelines_202502_blockchain_en.pdf.

([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 a 910/2014/EU rendeletnek a minősített elektronikus főkönyvekre vonatkozó referenciaszabványok és specifikációk tekintetében történő alkalmazására vonatkozó szabályok megállapításáról szóló végrehajtási rendelet tervezetével kapcsolatban.

MELLÉKLET

A minősített megosztott elektronikus főkönyvekre vonatkozó technikai specifikációk és referencia-szabványok jegyzéke

1. E rendelet alkalmazásában az alábbi fogalommeghatározások alkalmazandók:

   a) „véglegesség”: az elektronikus főkönyv adatrekordjának azon állapota, amelyben az visszafordíthatatlanná vált, és nem módosítható vagy nem távolítható el;

   b) „megosztott elektronikus főkönyv”: megosztott elektronikus főkönyvi csomópontok csoportja között megosztott elektronikus főkönyv, amelyet konszenzusos mechanizmus alkalmazásával szinkronizálnak a megosztott elektronikus főkönyvi csomópontok között;

   c) „megosztott elektronikus főkönyvi csomópont”: megosztott elektronikus főkönyvi hálózat részét képező olyan eszköz vagy folyamat, amely egy elektronikus főkönyv adatrekordjainak teljes vagy részleges másolatát tárolja;

   d) „megosztott elektronikus főkönyvi hálózat”: megosztott elektronikus főkönyvi csomópontok hálózata, amely megosztott elektronikus főkönyvi rendszert alkot;

   e) „megosztott elektronikus főkönyvi rendszer”: megosztott elektronikus főkönyvet megvalósító rendszer;

   f) „konszenzus”: a megosztott elektronikus főkönyvi csomópontok közötti megegyezés a tranzakciók érvényességéről, valamint a validált tranzakciók konzisztens és rendezett sorozatának fenntartásáról a megosztott elektronikus főkönyvi rendszerben;

   g) „konszenzusos mechanizmus”: azon szabályok és eljárások összessége, amelyek révén konszenzus érhető el;

   h) „irányadó szabályok”: azon protokollok, szabályzatok és mechanizmusok összessége, amelyek meghatározzák a megosztott elektronikus főkönyvi rendszer működésmódját, az adatok validálásának mikéntjét és elektronikus főkönyvbe való felvételi módját, valamint a résztvevők közötti interakció menetét;

   i) „tranzakció”: az elektronikus főkönyvön belüli munkafolyamat legkisebb egysége;

   j) „munkafolyamat”: az elektronikus főkönyv irányadó szabályainak megfelelő eredmény eléréséhez szükséges egy vagy több műveletsor;

   k) „validált tranzakció”: olyan tranzakció, amelynek esetében a megosztott elektronikus főkönyvi rendszer irányadó szabályaival összhangban ellenőrizték az előírt integritási, hitelességi és protokollspecifikus feltételeket;

   l) „kriptográfiai hivatkozás”: olyan adatokra való hivatkozás, amelyet arra alkalmas kriptográfiai technikákkal hoztak létre a hivatkozott adatok integritásának, hitelességének vagy nyomonkövethetőségének és az adatrekordok helyes sorrendjének biztosításához;

   m) „főkönyvi kivonat”: egy elektronikus főkönyv adatrekordjaiból származó, ellenőrizhető információk strukturált megjelenítése, amely áttekintést nyújt konkrét tevékenységekről, állapotokról vagy az előre meghatározott szabályoknak való megfelelésről;

   n) „minősített elektronikus főkönyvet vezető szolgáltató”: olyan minősített bizalmi szolgáltató, amelynek minősített bizalmi szolgáltatása minősített elektronikus főkönyvben történő adatrögzítést tartalmaz;

   o) „minősített megosztott elektronikus főkönyv”: olyan megosztott elektronikus főkönyv, amely megfelel a minősített elektronikus főkönyvre vonatkozó követelményeknek.

2. Amennyiben a minősített bizalmi szolgáltatónak főkönyvi kivonatot kell készítenie, ezt automatizált módon kell végeznie.

3. A minősített elektronikus főkönyvet vezető szolgáltatók minősített elektronikus főkönyvet hoznak létre, aktualizálnak és tartanak fenn, valamint elektronikus adatokat rögzítenek benne, a következőkben meghatározott specifikációknak megfelelően:

   a) A minősített elektronikus főkönyvet vezető minden szolgáltató esetében az ETSI EN 319 401 v3.1.1 (2024-06) szabvány, a következő kiigazításokkal:

      — 2.1. Normatív hivatkozások:

        [1] Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms” (Elfogadott kriptográfiai mechanizmusok), az Európai Uniós Hálózat- és Információ-biztonsági Ügynökség (ENISA) kiadványa

[2] IETF RFC 7515 (2015. május): „JSON Web Signature (JWS)” (JSON-webaláírások)

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

[4] 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

[5] 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

[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)

— 6.1. A bizalmi szolgáltatásra vonatkozó alkalmazási nyilatkozat:

  — REQ-6.1-12 Az elektronikus főkönyvre vonatkozó alkalmazási nyilatkozatnak legalább a következő információkat kell tartalmaznia:

    — az elektronikus főkönyvi platform funkcionális és technikai képességei, valamint használata a minősített elektronikus főkönyvben történő adatrögzítés mint minősített bizalmi szolgáltatás nyújtása során

    — a szolgáltatás nyújtása során az adatok eredetének hitelesítésére használt konkrét mechanizmusok

    — a szolgáltatás nyújtása során a szekvenciális időrendi sorrend meghatározására használt konkrét mechanizmusok

    — adott esetben az adatrekordok sorrendjének biztosítására használt kriptográfiai hivatkozás

    — adott esetben a főkönyvben tárolt adatrekordok és tranzakciók véglegességét és integritását biztosító konszenzusos mechanizmus, beleértve a véglegesség és az integritás eléréséig tartó biztonsági időszakot is

    — a szolgáltatás nyújtása során az adatok integritásának biztosítására használt konkrét mechanizmusok

  — 6.2. Szerződési feltételek:

    — REQ-6.2-03 A bizalmi szolgáltatást igénybe vevő előfizetőket és feleket a szerződéskötést megelőzően közérthetően, teljeskörűen és könnyen hozzáférhető formában, nyilvánosan elérhető helyen és egyénileg tájékoztatni kell a pontos szerződési feltételekről, beleértve a fent felsorolt elemeket

  — 6.3. Információbiztonsági szabályzat:

    — REQ-6.3-04X A bizalmi szolgáltató (TSP) eljárásokat dolgoz ki annak érdekében, hogy az üzleti követelményekkel és a vonatkozó jogszabályokkal és egyéb rendelkezésekkel összhangban értesítse a felügyeleti szervet a bizalmi szolgáltatás nyújtásában bekövetkező változásokról. A TSP a következők szerint értesíti a felügyeleti szervet:

      — legalább egy hónappal a változtatások végrehajtása előtt

      — legalább három hónappal a bizalmi szolgáltatás nyújtásának tervezett megszüntetése előtt

  — 7.2. Emberi erőforrások:

    — REQ-7.2-04X A TSP bizalmi szerepet betöltő személyzete képes teljesíteni a formális képzés és bizonyítványok, illetve a tényleges szakmai tapasztalat, vagy pedig a kettő kombinációja révén szerzett szaktudásra, tapasztalatra és képesítésre vonatkozó követelményt

— REQ-7.2-05X Ez magában foglalja az új fenyegetésekre és a jelenlegi biztonsági gyakorlatokra vonatkozó rendszeres (legalább 12 havonta történő) tájékoztatást

— 7.5. Kriptográfiai ellenőrzések:

— REQ-7.5-01X 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-7.5-02 Bizalmi szolgáltatásainak nyújtása céljára a TSP az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [1] kompatibilis, megfelelő kriptográfiai technikákat választ és alkalmaz

Konkrétan:

— REQ-7.5-03 A minősített elektronikus főkönyvet vezető szolgáltatók megállapítják az elektronikus főkönyvben szereplő adatrekordok eredetét. E célból a következő szabványoknak és specifikációknak megfelelően a szolgáltatás felhasználói által létrehozott, minősített tanúsítványokon alapuló, fokozott biztonságú elektronikus aláírásokat vagy az említett módon létrehozott, minősített tanúsítványokon alapuló, fokozott biztonságú elektronikus bélyegzőket használnak:

a) ETSI EN 319 122-1 V1.3.1 (2023-06). Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures [Elektronikus aláírások és infrastruktúrák (ESI). CAdES digitális aláírások. 1. rész: Építőelemek és CAdES-alapprofil-aláírások];

b) ETSI EN 319 132-1 V1.3.1 (2024-07). Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures [Elektronikus aláírások és bizalmi infrastruktúrák (ESI). XAdES digitális aláírások. 1. rész: Építőelemek és XAdES-alapprofil-aláírások];

c) ETSI TS 119 182-1 V1.2.1 (2024-07). Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures [Elektronikus aláírások és bizalmi infrastruktúrák (ESI). JAdES digitális aláírások. 1. rész: Építőelemek és JAdES-alapprofil-aláírások], a következő kiigazításokkal:

— 5.1.8. Az x5c (X.509 tanúsítványlánc) fejlécparaméter

— Az IETF RFC 7515 szabvány [2] 4.1.6. szakaszában meghatározott x5c fejlécparaméternek szerepelnie kell a JAdES-aláírásban, vagy aláírt, vagy alá nem írt fejlécparaméterként

— Az x5c fejlécparaméternek az IETF RFC 7515 szabvány [2] 4.1.6. szakaszában meghatározott szemantikájúnak kell lennie

— Az x5c fejlécparaméternek az IETF RFC 7515 szabvány [2] 4.1.6. szakaszában meghatározott szintaktikájúnak kell lennie

— REQ-7.5-04: A minősített elektronikus főkönyvet vezető szolgáltatók garantálják az elektronikus főkönyvben szereplő adatrekordok egyedi szekvenciális időrendi sorrendjét. E célból hash-listákon vagy hash-fákon alapuló kriptográfiai hivatkozásokat használnak kriptográfiai hasítófüggvények alkalmazásával, a következő specifikációknak és szabványoknak megfelelően:

a) SHA-256 vagy nagyobb kimeneti hash-méret, az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [1] összhangban;

b) SHA3-256 vagy nagyobb kimeneti hash-méret, az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [1] összhangban.

Alternatív megoldásként, amikor az elektronikus főkönyvben szereplő adatrekordok egyedi szekvenciális időrendi sorrendjének biztosítása érdekében időregisztrálást alkalmaznak, a minősített elektronikus főkönyvet vezető szolgáltatóknak minősített időbélyegzőket kell használniuk.

— REQ-7.5-05 A minősített elektronikus főkönyvet vezető szolgáltatók garantálják a minősített elektronikus főkönyvben rögzített adatrekordok integritását. E célból minősített tanúsítványokon alapuló, fokozott biztonságú elektronikus aláírásokat vagy minősített tanúsítványokon alapuló, fokozott biztonságú elektronikus bélyegzőket használnak a következő szabványoknak és specifikációknak megfelelően:

  a) bármely aláírás- vagy bélyegzőformátum, amely megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [1];

  b) SHA-256 vagy nagyobb kimeneti hash-méret, az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [1] összhangban;

  c) SHA3-256 vagy nagyobb kimeneti hash-méret, az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [1] összhangban;

  d) a minősített elektronikus főkönyvet vezető szolgáltatók garantálják, hogy a minősített elektronikus főkönyvben rögzített adatok bármely későbbi változása azonnal észlelhető legyen.

— REQ-7.5-06 Digitális aláírási mechanizmus használata esetén a minősített elektronikus főkönyvet vezető szolgáltató személyes aláírási kulcsait 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 ([1]) [6] 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) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) ([2]) ([3]) [4][5], EAL 4 vagy magasabb szintű tanúsítással; vagy

  c) 2030.12.31.-ig a FIPS PUB 140-3 szabvány ([4]) [3] 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 tanúsítással [4][5] rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják.

([1]) 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]) 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/2024/482/2025-01-08).

([3]) 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).

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

— 7.8. Hálózatbiztonság:

— REQ-7.8-14X A REQ-7.8-13 követelményben előírt sebezhetőségi vizsgálatot negyedévente legalább egyszer elvégzik

— REQ-7.8-18X A REQ-7.8-17X követelményben előírt behatolási tesztelést évente legalább egyszer elvégzik

— REQ-7.8-21X A tűzfalakat is úgy konfigurálják, hogy megakadályozzák a TSP működéséhez nem szükséges protokollok használatát és hozzáférést

— 7.9.1. Nyomon követés és naplózás:

— REQ-7.9.1-02X A nyomonkövetési tevékenységek során figyelembe veszik az összegyűjtött vagy elemzett információk érzékenységét

— 7.12. A szolgáltatás TSP általi megszüntetése és a szolgáltató szolgáltatásmegszüntetési tervei:

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

b) Emellett a megosztott elektronikus főkönyvi technológiákat alkalmazó, minősített elektronikus főkönyvet vezető minden szolgáltató esetében:

1. ISO 23257:2022 Blokklánc és megosztott főkönyvi technológiák – Referenciaarchitektúra, 9. szakasz, teljeskörű leírást nyújtva a megosztott elektronikus főkönyvi technológiai rendszerről, a megfelelő megosztott elektronikus főkönyvi technológiai hálózatról és a megosztott elektronikus főkönyvi technológiai csomópontokról;

2. ISO/TS 23635:2022 Blokklánc és megosztott főkönyvi technológiák – Iránymutatások az irányításhoz, az általa nyújtott elektronikus főkönyvi szolgáltatás irányítási struktúrájával kapcsolatos írásbeli és nyilvánosan hozzáférhető szabályzatokra és gyakorlatokra vonatkozóan.