2025/1550

2025.7.29.

A BIZOTTSÁG (EU) 2025/1550 VÉGREHAJTÁSI RENDELETE

(2025. július 28.)

az (EU) 2023/1543 európai parlamenti és tanácsi rendeletben említett decentralizált informatikai rendszerre vonatkozó műszaki előírások és egyéb követelmények megállapításáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról szóló 2023. július 12-i (EU) 2023/1543 európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 25. cikke (1) bekezdésének a), b), c) és d) pontjára,

mivel:

(1) Az (EU) 2023/1543 rendeletben említett decentralizált informatikai rendszer létrehozása érdekében meg kell határozni és el kell fogadni az említett rendszer megvalósítására vonatkozó műszaki előírásokat, intézkedéseket és célokat.

(2) Az (EU) 2023/1543 rendelet szerint a decentralizált informatikai rendszernek a tagállamok és az uniós ügynökségek és szervek informatikai rendszereiből, valamint kölcsönösen átjárható e-CODEX hozzáférési pontokból kell állnia, amelyeken keresztül ezek az informatikai rendszerek összekapcsolódnak. Ennek megfelelően a decentralizált informatikai rendszer műszaki előírásainak és egyéb követelményeinek tükrözniük kell ezt a keretet.

(3) Az (EU) 2023/1543 rendelettel összhangban a decentralizált informatikai rendszer hozzáférési pontjainak az (EU) 2022/850 európai parlamenti és tanácsi rendelet 3. cikkének (3) bekezdésében meghatározott engedélyezett e-CODEX hozzáférési pontokon kell alapulniuk ([2]).

(4) A tagállamok dönthetnek úgy, hogy a Bizottság által kifejlesztett referenciaimplementációt használják háttérrendszerként a nemzeti informatikai rendszer helyett. Az interoperabilitás biztosítása érdekében mind a nemzeti informatikai rendszereknek, mind a referenciaimplementációnak az e rendeletben meghatározott műszaki előírásokat és követelményeket kell teljesíteniük.

(5) A decentralizált informatikai rendszer kapacitásával és megbízhatóságával kapcsolatos esetleges technikai problémák enyhítése érdekében meg kell határozni az e rendszeren keresztül továbbított elektronikus bizonyítékok volumenére vonatkozó küszöbértéket. A rendszer elindítását követően nyomon kell követni az ilyen adattovábbítások gyakoriságát és volumenét, és adott esetben ki kell igazítani a küszöbértéket a rendszer hatékonyságának maximalizálása érdekében.

(6) A decentralizált informatikai rendszer interoperabilitásának és hatékonyságának javítása érdekében megbízást kell adni a megfelelő ETSI-szabványok alkalmazására. A jövőbeli fejlesztéseket nyomon kell követni, és szükség esetén mérlegelni kell további ETSI-szabványok elfogadását.

(7) Írországra nézve az (EU) 2023/1543 rendelet kötelező, ezért részt vesz e rendelet elfogadásában.

(8) Az Európai Unióról szóló szerződéshez, valamint az Európai Unió működéséről szóló szerződéshez csatolt, Dánia helyzetéről szóló 22. jegyzőkönyv 1. és 2. cikkével összhangban e rendelet Dániára nem kötelező és nem alkalmazandó.

([1]) HL L 191., 2023.7.28., 118. o., ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

([2]) Az Európai Parlament és a Tanács (EU) 2022/850 rendelete (2022. május 30.) a polgári és büntetőügyekben folytatott igazságügyi együttműködés területén történő, határokon átnyúló elektronikus adatcserére szolgáló számítógépes rendszerről (e-CODEX-rendszer) és az (EU) 2018/1726 rendelet módosításáról (HL L 150., 2022.6.1., 1. o., ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([3]) 42. cikkének (1) bekezdésével összhangban a Bizottság egyeztetett az európai adatvédelmi biztossal, aki 2025. június 25-én véleményt nyilvánított.

(10) Az e rendeletben előírt intézkedések összhangban vannak az (EU) 2023/1543 rendelet 26. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

A decentralizált informatikai rendszerre vonatkozó műszaki előírások

Az (EU) 2023/1543 rendelet 25. cikkének (1) bekezdésében említett decentralizált informatikai rendszernek az említett rendelet 19. cikke szerinti kommunikációra vonatkozó műszaki előírásait és követelményeit, intézkedéseit és célkitűzéseit e rendelet melléklete határozza meg.

2. cikk

Hatálybalépés

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

Ez a rendelet a Szerződéseknek megfelelően teljes egészében kötelező és közvetlenül alkalmazandó a tagállamokban.

Kelt Brüsszelben, 2025. július 28-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

([3]) 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 DECENTRALIZÁLT INFORMATIKAI RENDSZERRE VONATKOZÓ MŰSZAKI ELŐÍRÁSOK

(az 1. cikkben említettek szerint)

1. **Bevezetés és alkalmazási kör**

Ez a melléklet az (EU) 2023/1543 rendelet szerinti eljárások lefolytatására szolgáló decentralizált informatikai rendszerre vonatkozó műszaki előírásokat, intézkedéseket és célokat rögzíti.

Az (EU) 2023/1543 rendelet és különösen annak 19. cikke szerint a decentralizált informatikai rendszernek lehetővé kell tennie az írásbeli kommunikációt az illetékes hatóságok és a kijelölt telephelyek vagy jogi képviselők között, az illetékes hatóságok között, valamint az illetékes hatóságok és az illetékes uniós ügynökségek vagy szervek között.

2. **Fogalommeghatározások**

2.1. „Hypertext Transfer Protocol Secure” vagy „HTTPS”: titkosított kommunikációs és biztonságos kapcsolódási csatornák;

2.2. „eredet letagadhatatlansága”: azon intézkedések, amelyek igazolják az adatok integritását és eredetét olyan módszerek segítségével, mint a digitális tanúsítás, a nyilvános kulcsú infrastruktúra, az elektronikus aláírások és az elektronikus bélyegzők;

2.3. „beérkezés letagadhatatlansága”: azon intézkedések, amelyek igazolják a kibocsátó számára az adatok meghatározott címzetthez történő beérkezését olyan módszerek segítségével, mint a digitális tanúsítás, a nyilvános kulcsú infrastruktúra, az elektronikus aláírások és az elektronikus bélyegzők;

2.4. „egyszerű objektumelérési protokoll”: a World Wide Web Konzorcium szabványainak megfelelő olyan üzenetküldő protokollra vonatkozó előírás, amely a webszolgáltatások számítógépes hálózatokon belüli megvalósítására vonatkozó strukturált információ cseréjéhez alkalmazandó;

2.5. „Representational State Transfer” (REST): a hálózatba kapcsolt alkalmazások tervezésére szolgáló architektúrastílus, amely állapotfüggetlen kliens-szerver kommunikációs modellre támaszkodik, és szabványos módszerekkel végez műveleteket a jellemzően strukturált formátumú erőforrásokon;

2.6. „webszolgáltatás”: olyan szoftverrendszer, amelynek célja az együttműködő gépek közötti kapcsolat támogatása egy adott hálózaton belül, és amely géppel feldolgozható formátumban leírt interfésszel rendelkezik;

2.7. „adatcsere”: üzenetek, formanyomtatványok, iratok és elektronikus bizonyítékok cseréje a decentralizált informatikai rendszeren keresztül;

2.8. „API”: közös adatcsere-szabványon alapuló alkalmazásprogramozási interfész, amely lehetővé teszi az elektronikus bizonyítékok iránti kérelmekkel kapcsolatos információk és adatok cseréje céljából egyedi informatikai megoldásokat alkalmazó szolgáltatók számára, hogy automatizált eszközökkel hozzáférjenek a decentralizált informatikai rendszerekhez;

2.9. „webalapú interfész”: az interneten HTTPS-en keresztül elérhető felhasználói felület, amely lehetővé teszi a szolgáltatók számára, hogy manuálisan hozzáférjenek a decentralizált informatikai rendszerhez a hatóságokkal való biztonságos kommunikáció, valamint az elektronikus bizonyítékok iránti kérelmekkel kapcsolatos információk és adatok cseréje érdekében anélkül, hogy erre a célra saját külön infrastruktúrát kellene létrehozniuk;

2.10. „ETSI-szabványok”: az Európai Távközlési Szabványügyi Intézet (ETSI) által az információs és kommunikációs technológiák interoperabilitásának, biztonságának és hatékonyságának biztosítása érdekében kidolgozott műszaki előírások és szabványok. Kereteket, protokollokat és bevált gyakorlatokat biztosítanak a technológiák széles köréhez, beleértve a mobilhálózatokat, a rádiókommunikációt, a kiberbiztonságot és az internetes infrastruktúrát;

2.11. „hash kivonat”: a tetszőleges hosszúságú bemenetre alkalmazott kriptográfiai hash-függvény által generált, rögzített hosszúságú kimenet. A kriptográfiai hash-függvényt úgy tervezték, hogy rendelkezzen az alapvető biztonsági tulajdonságokkal, beleértve a preimage támadással szembeni ellenállást, a második preimage támadással szembeni ellenállást és az ütközés-ellenállóságot, amely biztosítja az inverziós és ütközéses támadásokkal szembeni robusztusságát;

2.12. „e-CODEX-rendszer”: az (EU) 2022/850 rendelet 3. cikkének (1) bekezdésében meghatározott e-CODEX-rendszer;

2.13. „uniós e-igazságügyi alapszókészlet”: az (EU) 2022/850 rendelet mellékletének 4. pontjában meghatározott uniós e-igazságügyi alapszókészlet;

2.14. „ebMS”: az OASIS keretrendszerben kidolgozott ebXML üzenetküldő szolgáltatás, amely lehetővé teszi az elektronikus üzleti dokumentumok SOAP protokollon keresztül történő biztonságos, megbízható és interoperábilis cseréjét, támogatva a vállalkozások közötti integrációt a különböző rendszerekben;

2.15. „AS4”: 4. alkalmazhatósági nyilatkozat, az ebMS 3.0 profilját képező OASIS szabvány, amely leegyszerűsíti a vállalkozások közötti biztonságos és interoperábilis üzenetküldést olyan nyílt szabványok alkalmazásával, mint a SOAP és a WS-Securtiy;

2.16. „helyreállítási időre vonatkozó célkitűzés”: biztonsági eseményt követően a szolgáltatás helyreállításának maximális elfogadható ideje;

2.17. „helyreállítási pontra vonatkozó célkitűzés”: az adatvesztés maximális elfogadható mennyisége meghibásodás esetén.

3. **Az elektronikus eszközök útján történő kommunikáció módjai**

3.1. A tagállamok illetékes hatóságai, az illetékes hatóságok és a szolgáltatók kijelölt telephelyei vagy jogi képviselői, valamint az illetékes hatóságok és az uniós ügynökségek vagy szervek közötti írásbeli kommunikáció céljából a decentralizált informatikai rendszer szolgáltatásalapú kommunikációs módszereket, például webszolgáltatásokat vagy más újrafelhasználható komponenseket és szoftvermegoldásokat alkalmaz adatcsere céljából. Ez konkrétan az (EU) 2022/850 rendelet 5. cikkének (2) bekezdésében meghatározott e-CODEX hozzáférési pontokon keresztüli kommunikációt jelenti. Ezért a hatékony és interoperábilis, határokon átnyúló adatcsere biztosítása érdekében a decentralizált informatikai rendszernek támogatnia kell az e-CODEX-rendszeren keresztüli kommunikációt.

3.2. Tekintettel az (EU) 2023/1543 rendelet 19. cikkének (1) és (4) bekezdésében meghatározott decentralizált informatikai rendszeren keresztül a közlésre kötelező európai határozat nyomán továbbítandó elektronikus bizonyítékok várható nagy mennyiségére, ami olyan technikai kapacitásbeli korlátokhoz vezethet, amelyek negatívan befolyásolhatják a decentralizált informatikai rendszert, az elektronikus bizonyítékok legfeljebb 25 MB (25 600 kb) küszöbértékig továbbíthatók a rendszeren keresztül. A fenti küszöbértéket meghaladó elektronikus bizonyítékok továbbítása az említett rendelet 19. cikkének (5) bekezdésével összhangban történik.

3.3. Tekintettel az (EU) 2023/1543 rendelet 19. cikkének (6) bekezdésére, amennyiben a továbbítás az említett bekezdésben előírt alternatív módon történik, mert az említett rendelet 19. cikkének (5) bekezdésében meghatározott okok valamelyike miatt a decentralizált informatikai rendszer nem használható:

3.3.1. Amennyiben a továbbítás az illetékes hatóságok és az (EU) 2023/1543 rendelet 19. cikkének (1) bekezdése szerinti szolgáltatók közötti írásbeli kommunikációt érint, beleértve a formanyomtatványok cseréjét is, a továbbítás kezdeményezője rögzíti a továbbítást a decentralizált informatikai rendszer részét képező nemzeti informatikai rendszerében. A rögzített információ tartalmazza legalább az ügy vagy az ügyirat hivatkozási számát, a továbbítás dátumát és időpontját, a feladót és a címzettet, a fájl nevét és méretét.

3.3.2. Amennyiben a továbbítás az illetékes hatóságok közötti írásbeli kommunikációt – többek között formanyomtatványok cseréjét –, valamint az (EU) 2023/1543 rendelet 19. cikkének (4) bekezdése szerinti illetékes uniós ügynökségekkel vagy szervekkel folytatott írásbeli kommunikációt érint, a továbbítás kezdeményezője rögzíti a továbbítást a decentralizált informatikai rendszerben – az annak részét képező nemzeti informatikai rendszerben vagy adott esetben az illetékes uniós ügynökség vagy szerv által működtetett informatikai rendszerekben. A rögzített információ tartalmazza legalább az ügy vagy az ügyirat hivatkozási számát, a továbbítás dátumát és időpontját, a feladót és a címzettet, a fájl nevét és méretét.

3.3.3. Amennyiben a közlésre kötelező európai határozat szerinti elektronikus bizonyíték továbbítása a szolgáltatók és a kibocsátó állam illetékes hatóságai között alternatív kommunikációs módon történt ([1]), vagy amennyiben az elektronikus bizonyítékot a végrehajtó hatóság alternatív módon továbbította a kibocsátó állam illetékes hatóságainak az (EU) 2023/1543 rendelet 16. cikkének (9) bekezdésében előírt végrehajtási eljárás keretében, a kibocsátó:

a) a manifeszt állományban rögzíti és továbbítja a következő információkat annak a hatóságnak, amelynek számára az elektronikus bizonyítékot továbbították vagy hozzáférhetővé tették:

1. a feladóra és a címzettre vonatkozó információk;

2. a benyújtott elektronikus bizonyítékokat egy adott közlésre kötelező vagy megőrzésre kötelező európai határozat(ok)hoz társító metaadatok;

3. a továbbítás dátuma és időpontja, vagy annak feltüntetése, hogy az elektronikus bizonyítékot mikor bocsátották a címzett rendelkezésére;

4. a továbbítás módjára vonatkozó információk (pl. az elektronikus bizonyíték rendelkezésre bocsátására szolgáló biztonságos kapcsolatról nyilvántartott adat, az átvétel vagy kézbesítés postai szolgáltató általi igazolása stb.) ([2]);

5. a kibocsátó államban a szándékolt címzett számára továbbított vagy más módon hozzáférhetővé tett elektronikus bizonyíték teljes fájlneve(i);

6. a kibocsátó államban a szándékolt címzett számára továbbított vagy más módon hozzáférhetővé tett elektronikus bizonyíték adatmérete;

7. a továbbított vagy hozzáférhetővé tett adatok legalább egy hash kivonata, a felhasznált hash algoritmus(ok) megjelölésével. A hash kivonat kiszámításához használt hash algoritmus kriptográfiailag erős, általánosan használt algoritmus, amely ellenálló a nyilvánosan közzétett gyengeségekkel, például az ütközéssel szemben (SHA-512, SHA3–512, BLAKE2 vagy RIPEMD-160, de a technológiai fejlődéstől függően akár ezeknél erősebb);

b) adott esetben az a) pontban említett manifeszt állományban feltünteti azt a dátumot és időpontot, ameddig az elektronikus bizonyíték hozzáférhető marad. Az időtartamot észszerűen kell meghatározni úgy, hogy az alatt a kibocsátó állam illetékes hatósága lekérhesse az elektronikus bizonyítékot; ez az elektronikus bizonyíték rendelkezésre bocsátásától számított legalább 10 és legfeljebb 45 naptári nap. A kibocsátó állam illetékes hatóságának kérésére a kibocsátó által megjelölt időtartam egyedi esetben meghosszabbítható;

c) a fenti a) pontban említett manifeszt állományban rögzíthet és továbbíthat az üggyel kapcsolatos bármely további információt vagy megjegyzést annak a hatóságnak, amelynek számára az elektronikus bizonyítékot továbbították vagy hozzáférhetővé tették.

3.4. Tekintettel az (EU) 2023/1543 rendelet 28. cikkére, a referenciaimplementáció programozottan gyűjti, továbbítja vagy más módon hozzáférhetővé teszi az említett cikk (2) bekezdésében felsorolt statisztikákat strukturált (pl. XML) és strukturálatlan (pl. PDF) adatformátumokban egyaránt. Az (EU) 2023/1543 rendelet 28. cikkének (3) bekezdésével összhangban a tagállamok által működtetett nemzeti portálok ([3]) – megfelelő műszaki felszereltségük esetén – automatizált folyamat keretében is továbbíthatják vagy szolgáltathatják ezeket a statisztikákat a Bizottságnak. A Bizottság iránymutatást ad ki az adatstruktúráról, valamint e statisztikák gyűjtésének és közlésének módszeréről.

([1]) Az egyértelműség kedvéért az illetékes nemzeti hatóságokra való hivatkozásokat értelemszerűen úgy kell értelmezni, hogy azok az Eurojust nemzeti tagjaira, az európai ügyészekre és a delegált európai ügyészekre is vonatkoznak, amennyiben az uniós jog és a nemzeti jog alapján felhatalmazással rendelkeznek ugyanazon feladatok ellátására.

([2]) Emlékeztetni kell arra, hogy a 19. cikk (5) bekezdésével összhangban az ilyen alternatív kommunikációs módon történő továbbításnak meg kell felelnie a gyors, biztonságos és megbízható jelleg követelményeinek, lehetővé téve a címzett számára a hitelesség megállapítását.

([3]) „Nemzeti portálok” alatt az (EU) 2023/1543 rendelet 3. cikkének 21. pontjában meghatározott decentralizált informatikai rendszer részét képező nemzeti „informatikai rendszerek” értendők.

4. **Kommunikációs protokollok**

4.1. A decentralizált informatikai rendszer biztonságos internetes protokollokat használ a következőkhöz:

a) kommunikáció az illetékes hatóságok között a decentralizált informatikai rendszeren belül;

b) kommunikáció az illetékes hatóságok, valamint az uniós ügynökségek és szervek között a decentralizált informatikai rendszeren belül;

c) kommunikáció az illetékes hatóságok és a szolgáltatók között API-n és webalapú interfészen keresztül; valamint

d) kommunikáció a bírósági adatbázissal.

4.2. A strukturált adatok és metaadatok meghatározása és továbbítása tekintetében a decentralizált informatikai rendszer komponensei átfogó és széles körben elfogadott ágazati szabványokon és protokollokon (például SOAP, REST), kiemelten az európai szabványügyi szervezetek, például az ETSI által hivatkozott szabványokon és protokollokon alapulnak.

4.3. Az átviteli és üzenetküldési protokollok tekintetében a decentralizált informatikai rendszer biztonságos szabványalapú protokollokon alapul, például:

a) a határokon átnyúló adatcseréhez AS4 profil, amely titkosítás és letagadhatatlanság mellett biztosítja a biztonságos és megbízható üzenetküldést;

b) a JSON és XML formátumokat támogató kommunikációhoz HTTPS/RESTful API-k;

c) a nagy megbízhatóságú interakciókhoz SOAP, ezen belül a hitelesítéshez és a titkosításhoz WS-Security.

4.4. A zökkenőmentes és interoperábilis adatcsere érdekében a decentralizált informatikai rendszer által használt kommunikációs protokoll megfelel a vonatkozó interoperabilitási szabványoknak.

4.5. Az elektronikus bizonyítékok XML sémái adott esetben olyan vonatkozó szabványokat vagy szókészleteket használnak, amelyek az e séma keretében meghatározott elemek és típusok megfelelő validálásához szükségesek. Ezek az alábbiak lehetnek:

a) az uniós e-igazságügyi alapszókészlet;

b) nem minősített adattípusok;

c) európai uniós nyelvkódlista.

Emellett adott esetben az XML-sémák tartalmazhatják a vonatkozó ETSI-szabványokat azok definícióinak alkalmazása érdekében.

4.6. A Bizottság meghatározza a közös API-ra vonatkozó előírásokat, amelyet a végrehajtó államok a decentralizált informatikai rendszerhez való hozzáférés eszközeként a szolgáltatók rendelkezésére bocsátanak. A lehetséges és észszerű mértékben az API az ETSI TS 104 144 szabványon (az elektronikus bizonyítékokról szóló (EU) 2023/1543 rendeletnek a nemzeti hatóságokra és szolgáltatókra vonatkozó interfészdefinícióján) alapul.

4.7. A biztonsági és hitelesítési protokollok esetében a decentralizált informatikai rendszer szabványokon alapuló protokollokra épül, például:

a) a hálózatokon keresztül történő titkosított és hitelesített kommunikációhoz TLS (Transport Layer Security), a kölcsönös hitelesítés X.509 digitális tanúsítványokon keresztüli támogatásával;

b) a biztonságos hitelesítéshez és engedélyezéshez OAuth/OpenID Connect (OIDC);

c) a biztonságos kulcscseréhez és üzenetintegritás-ellenőrzéshez nyilvános kulcsú infrastruktúra és digitális aláírások, megbízható tanúsító hatóságok által kiadott digitális tanúsítványok (X.509) használatával.

5. **Információbiztonsági célkitűzések és a vonatkozó műszaki intézkedések**

5.1. A decentralizált informatikai rendszeren keresztül történő információcsere tekintetében az információtechnológiai biztonsági minimumkövetelmények betartását biztosító műszaki intézkedések az alábbiakat foglalják magukban:

a) az információ bizalmas jellegét biztosító intézkedések, többek között biztonságos kommunikációs csatornák használata;

b) az adatok (üzenetek, formanyomtatványok, iratok és elektronikus bizonyítékok) sértetlenségének biztosítására irányuló intézkedések használaton kívül és továbbítás alatt;

c) a decentralizált informatikai rendszeren belül az információküldő eredetének letagadhatatlanságát és az információ beérkezésének letagadhatatlanságát biztosító intézkedések;

d) a szolgáltatásokhoz és adatokhoz való folyamatos hozzáférés biztosítása, valamint a kibertámadások vagy hibák miatti fennakadások megelőzése révén a hozzáférhetőséget biztosító intézkedések;

e) az információbiztonsági eseményeknek az információtechnológiai biztonsági előírásokra vonatkozó nemzetközi ajánlásokkal összhangban történő naplózását biztosító intézkedések;

f) a felhasználók hitelesítését és engedélyezését, valamint a decentralizált informatikai rendszerhez kapcsolódó rendszerek azonosságának ellenőrzését lehetővé tévő intézkedések;

5.2. A decentralizált informatikai rendszer komponensei biztosítják a biztonságos kommunikációt és adatátvitelt, ennek érdekében a hitelesítéshez és a biztonságos kulcscseréhez titkosítást és digitális tanúsítványokra épülő nyilvános kulcsú infrastruktúrát, az üzenetek bizalmas jellegének és integritásának fenntartása érdekében pedig biztonságos üzenetküldési protokollokat – AS4 (ebMS), RESTful API-k, SOAP – használnak.

5.3. A decentralizált informatikai rendszer komponenseit a beépített és alapértelmezett adatvédelem elvével összhangban kell fejleszteni, és megfelelő adminisztratív, szervezeti és technikai intézkedéseket kell végrehajtani a magas szintű kiberbiztonság biztosítása érdekében.

5.4. A Bizottság az (EU) 2018/1725 rendeletben meghatározott adatvédelmi követelményekkel és elvekkel összhangban megtervezi, fejleszti és karbantartja a referenciaimplementációt. A Bizottság által biztosított referenciaimplementáció lehetővé teszi a tagállamok számára az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([4]), illetve adott esetben az (EU) 2016/680 európai parlamenti és tanácsi irányelv ([5]) szerinti kötelezettségeik teljesítését.

5.5. Azok a tagállamok, amelyek a referenciaimplementációtól eltérő nemzeti informatikai rendszert használnak, végrehajtják az annak biztosításához szükséges intézkedéseket, hogy az megfeleljen az (EU) 2016/679 rendelet és adott esetben az (EU) 2016/680 irányelv követelményeinek.

5.6. Tekintettel a decentralizált informatikai rendszerben való részvételükre, az Eurojust és az Európai Ügyészség végrehajtja az annak biztosításához szükséges intézkedéseket, hogy informatikai rendszereik megfeleljenek az (EU) 2018/1725 rendelet és alapító jogi aktusaik követelményeinek.

5.7. A tagállamok, az Eurojust és az Európai Ügyészség a vonatkozó szakpolitikáikkal összhangban megbízható mechanizmusokat hoznak létre a fenyegetések észlelése és a biztonsági eseményekre való reagálás céljából, amelyekkel biztosítják a biztonsági események időben történő azonosítását, mérséklését és az azokat követő helyreállítást a decentralizált informatikai rendszer részét képező, felelősségi körükbe tartozó informatikai rendszerek tekintetében.

6. **Az elektronikus bizonyítékok** ([6]) **titkosítása**

6.1. A decentralizált informatikai rendszer által biztosított biztonsági intézkedések sérelme nélkül a közlésre kötelező európai határozat kibocsátásakor az illetékes hatóságok külön X.509 nyilvános tanúsítványt is kibocsáthatnak az elektronikus bizonyítékok aszimmetrikus titkosítása céljából.

([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.).

([5]) Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (HL L 119., 2016.5.4., 89. o.).

([6]) Az egyértelműség kedvéért az „elektronikus bizonyíték” kifejezés értelmezése az (EU) 2023/1543 rendelet 3. cikkének 8. pontjában szereplő fogalommeghatározásra korlátozódik.

6.2. A 6.1. szakaszban említett tanúsítványok kiállítása, kezelése, ellenőrzése és minden kapcsolódó szempontja, valamint a megfelelő nyilvános kulcsú infrastruktúra a kiállító állam kizárólagos felelőssége.

6.3. A jövőbeli technológiai fejlesztések sérelme nélkül a nyilvános tanúsítványok támogatják az olyan iparági standard titkosítási algoritmusokat, mint az RSA (Rivest–Shamir–Adleman), az ECDH (Elliptic Curve Diffie-Hellman), vagy az ECC (Elliptic Curve Cryptography).

6.4. A nyilvános tanúsítványok a megfelelő „keyUsage" kiterjesztéssel rendelkeznek, például az RSA-alapú tanúsítványok esetében a „keyEncipherment" vagy „dataEncipherment", az ECC-alapú tanúsítványok esetében pedig a „keyAgreement" kiterjesztéssel. A tanúsítványok PEM (Privacy-Enhanced Mail) vagy DER (Distinguiated Encoding Rules) formátumban állnak rendelkezésre.

6.5. Amennyiben a kibocsátó hatóság X.509 állami tanúsítványt bocsátott rendelkezésre, és a szolgáltató a közlésre kötelező európai határozat alapján küldi meg a közlendő elektronikus bizonyítékot, a szolgáltató, mielőtt a decentralizált informatikai rendszeren keresztül továbbítja az adatokat, a kibocsátó állam által rendelkezésre bocsátott vonatkozó X.509. számú nyilvános tanúsítvány felhasználásával titkosítja az elektronikus bizonyítékot.

6.6. Amennyiben a kiállító hatóság X.509 nyilvános tanúsítványt bocsátott rendelkezésre, azonban az elektronikus bizonyítékok titkosított formában történő továbbítása technikai vagy egyéb indokolt okok miatt nem lehetséges, akkor az (EU) 2023/1543 rendelet 19. cikkének (5) bekezdése szerinti rendelkezés sérelme nélkül a szolgáltató az adatokat tartalomtitkosítás nélkül is továbbíthatja. Ilyen esetekben a szolgáltató indokolással ellátott magyarázatot ad a kibocsátó hatóságnak.

7. **A rendszer által biztosított szolgáltatások hozzáférhetőségével kapcsolatos minimumcélok**

7.1. A tagállamok, az Eurojust és az Európai Ügyészség biztosítják, hogy a decentralizált informatikai rendszer felelősségi körükbe tartozó komponensei a hét minden napján 24 órában rendelkezésre álljanak, évente legalább 98 %-os műszaki rendelkezésreállási aránnyal, kivéve a tervezett karbantartást.

7.2. A Bizottság gondoskodik arról, hogy a bírósági adatbázis a hét minden napján 24 órában rendelkezésre álljon, évente 99 %-ot meghaladó műszaki rendelkezésreállási aránnyal, kivéve a tervezett karbantartást.

7.3. Lehetőség szerint munkanapokon a karbantartási műveleteket közép-európai idő szerint 20:00 és 7:00 óra közé kell ütemezni.

7.4. A tagállamok, az Eurojust és az Európai Ügyészség a következők szerint értesítik a Bizottságot és a többi tagállamot a karbantartási tevékenységekről:

a) 5 munkanappal korábban olyan karbantartási műveletek esetén, amelyek legfeljebb 4 órás hozzáférhetetlenséget okozhatnak;

b) 10 munkanappal korábban olyan karbantartási műveletek esetén, amelyek 4–12 órás hozzáférhetetlenséget okozhatnak;

c) 30 munkanappal korábban olyan karbantartási műveletek esetén, amelyek több mint 12 órás hozzáférhetetlenséget okozhatnak;

7.5. Amennyiben a tagállamok, az Eurojust vagy az Európai Ügyészség rögzített rendszeres karbantartási időszakokkal rendelkeznek, tájékoztatják a Bizottságot és a decentralizált informatikai rendszer résztvevőit ezen időszakok ütemezett napjáról és időpontjáról. A 7.4. szakaszban meghatározott kötelezettségektől eltérően amennyiben a decentralizált informatikai rendszer tagállamok, Eurojust vagy Európai Ügyészség felelősségi körébe tartozó komponensei a rögzített rendszeres karbantartási időszakok valamelyikében nem állnak rendelkezésre, a tagállamok dönthetnek úgy, hogy nem minden alkalommal értesítik a Bizottságot.

7.6. A decentralizált informatikai rendszer tagállamok, Eurojust vagy Európai Ügyészség felelősségi körébe tartozó komponenseinek váratlan műszaki meghibásodása esetén a tagállamok haladéktalanul tájékoztatják a Bizottságot és a decentralizált informatikai rendszer résztvevőit a hibáról, és amennyiben ismert, az elhárítás tervezett idejéről.

7.7. A decentralizált informatikai rendszer valamely tagállam felelősségi körébe tartozó komponenseit érintő karbantartási tevékenységek vagy váratlan műszaki meghibásodás esetén, amely kedvezőtlen hatással van az API és/vagy a webalapú interfész szolgáltatók általi elérhetőségére, az érintett tagállam haladéktalanul elérhetővé teszi ezeket az információkat egy weboldalon, és/vagy indokolatlan késedelem nélkül közli azokat a területén működő szolgáltatókkal.

7.8. A bírósági adatbázis váratlan műszaki meghibásodása esetén a Bizottság haladéktalanul tájékoztatja a tagállamokat, az Eurojustot és az Európai Ügyészséget a leállásról, és amennyiben ismert, az elhárítás tervezett idejéről.

7.9. A szolgáltatás zavara esetén a tagállamok, az Eurojust és az Európai Ügyészség biztosítják a szolgáltatás gyors helyreállítását és a minimális adatvesztést, összhangban a helyreállítási időre és a helyreállítási pontra vonatkozó célkitűzéssel.

7.10. A tagállamok, az Eurojust és az Európai Ügyészség megfelelő intézkedéseket hajtanak végre a fent vázolt rendelkezésreállási célkitűzések elérésére, és eljárásokat dolgoznak ki a biztonsági eseményekre való hatékony reagálás céljából.

8. **Illetékes hatósági/bírósági adatbázis (CDB)**

8.1. Tekintettel az (EU) 2023/1543 rendelet 19. cikkére, a decentralizált informatikai rendszer működéséhez elengedhetetlen a szolgáltatókra és az illetékes hatóságokra vonatkozó hiteles adatbázis létrehozása.

8.2. Az illetékes hatóságok hiteles adatbázisa strukturált formában tartalmazza a következő információkat:

a) az (EU) 2023/1543 rendelet 19. cikkének alkalmazásában az említett rendelet 31. cikke (1) bekezdésének a)–c) pontja szerint bejelentett illetékes hatóságokra vonatkozó információk, többek között a következők tekintetében:

1. az Eurojust nemzeti tagjai, annak feltüntetésével, hogy a nemzeti jog alapján jogosultak-e közlésre kötelező európai határozatok és megőrzésre kötelező európai határozatok kibocsátására az (EU) 2018/1727 európai parlamenti és tanácsi rendelet 8. cikkének (3) és (4) bekezdésével összhangban ([7]);

2. a delegált európai ügyészek és az európai ügyészek, amennyiben az (EU) 2017/1939 tanácsi rendelet ([8]) 105. cikkének (3) bekezdésével összhangban, az (EU) 2023/1543 rendelet értelmében vett illetékes kibocsátó hatóságként értesítést kapnak a tagállamoktól;

b) adott esetben a hatóságok illetékességi területének meghatározásához szükséges információk, vagy a hatáskörük megállapításához szükséges egyéb releváns kritériumok;

c) a decentralizált informatikai rendszeren belüli adatcserék megfelelő működéséhez és technikai üzenettovábbításához szükséges információk.

8.2.1. A 8.2. szakasz c) pontjában említett információk a következőket tartalmazzák:

a) a szolgáltató kijelölt telephelyének letelepedése, vagy jogi képviselőjének honossága szerinti tagállamra vonatkozó információk:

1. tagállam;

2. központi hatóság;

([7]) Az Európai Parlament és a Tanács (EU) 2018/1727 rendelete (2018. november 14.) az Európai Unió Büntető Igazságügyi Együttműködési Ügynökségéről (Eurojust) és a 2002/187/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről (HL L 295., 2018.11.21., 138. o.).

([8]) A Tanács (EU) 2017/1939 rendelete (2017. október 12.) az Európai Ügyészség létrehozására vonatkozó megerősített együttműködés bevezetéséről (HL L 283., 2017.10.31., 1. o.).

b) a szolgáltatóra vonatkozó információk:

1. név;
2. cím/székhely;
3. cégjegyzékszám;
4. társasági forma;
5. telefonszám;
6. e-mail-cím;

c) a kijelölt telephelyre/jogi képviselőre vonatkozó információk:

1. a jogalany típusa (kijelölt létesítmény/jogi képviselő);
2. név;
3. cím/székhely;
4. telefonszám;
5. e-mailcím;
6. általános kapcsolattartó személy/szervezet;
7. a szolgáltató/kijelölt telephely/jogi képviselő által elfogadott hivatalos nyelv(ek);
8. az Európai Parlament és a Tanács (EU) 2023/1544 irányelv ([9]) 2. cikkének 1. pontjában említett és az unióban nyújtott szolgáltatások;
9. azon uniós jogi eszközök típusa, amelyek tekintetében a kijelölt telephelyet kijelölték, illetve a jogi képviselőt kinevezték (akkor, ha a tagállamok nem vesznek részt az összes vonatkozó uniós jogi eszköz alkalmazásában);
10. kijelölés/kinevezés területi hatálya;

d) információ hitelesítése:

1. meghatalmazott képviselő neve;
2. beosztás;
3. cím;
4. telefonszám;
5. e-mail-cím;
6. dátum.

8.2.2. Amennyiben rendelkezésre állnak, a 8.2. szakasz c) pontjában említett információk a következőket foglalhatják magukban:

a) a szolgáltatóra vonatkozó információk:

1. az értesítésekkel kapcsolatos megkeresésekért felelős kapcsolattartó személy (amennyiben eltér az aláírótól);
2. weboldal;

b) a rendelkezésre álló adatok típusai:

1. minden érintett szolgáltatás esetében:

— a rendelkezésre álló adatok típusai,

— adatkategória,

— azonosítók,

— az adatok rendelkezésre állásának időtartama;

([9]) Az Európai Parlament és a Tanács (EU) 2023/1544 irányelve (2023. július 12.) a büntetőeljárásban az elektronikus bizonyítékok gyűjtése céljából a kijelölt telephelyek kijelöléséről és a jogi képviselők kinevezéséről szóló harmonizált szabályok meghatározásáról (HL L 191., 2023.7.28., 181. o., ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2. az adatokra vonatkozó kiegészítő információk;
3. a szolgáltatásra vonatkozó további információk (pl. alvállalkozói kapcsolatok);

c) a kijelölt telephelyre/jogi képviselőre vonatkozó információk:
1. egyéb szolgáltatók, amelyek tekintetében a kijelölt telephelyet vagy a jogi képviselőt kijelölték, illetve kinevezték;
2. technikai segítségnyújtás elérhetőségi adatai;
3. szükséghelyzeti kapcsolattartó;

d) technikai információk:
1. a műszaki kapcsolattartó pont neve;
2. a műszaki kapcsolattartó pont telefonszáma;
3. a műszaki kapcsolattartó pont e-mail-címe;
4. az API URL az adattípusokra vonatkozó információk dinamikus lekérdezéséhez;
5. a nemzeti informatikai rendszerhez való csatlakozás típusa:
— webalapú interfész,
— API,
— push API URL.

8.3. Tekintettel a decentralizált informatikai rendszer operatív igényeire:

a) a Bizottság felel a hiteles adatbázis fejlesztéséért, karbantartásáért, üzemeltetéséért és támogatásáért;

b) a Bizottság a decentralizált informatikai rendszerben való részvételük céljából az illetékes hatóságok, az Eurojust és az Európai Ügyészség rendelkezésére bocsátott API-n keresztül hozzáférést tesz lehetővé a hiteles adatbázishoz;

c) a tagállamok biztosítják, hogy az illetékes hatóságaikra vonatkozóan a hiteles adatbázisban szereplő, a 8.2. szakasz a) és b) pontjában meghatározott információk teljeskörűek, pontosak és naprakészek legyenek;

d) a hiteles adatbázis lehetővé teszi a tagállamok számára, hogy rendelkezésre bocsássák és frissítsék a szolgáltatóikra vonatkozó információkat, valamint a decentralizált informatikai rendszerben részt vevő hatóságok számára pedig ezen információk programozott elérését és lekérdezését;

e) a tagállamok és a szolgáltatók biztosítják, hogy a hiteles adatbázisban szereplő, a 8.2. szakasz c) pontjában meghatározott információk hiánytalanok, pontosak és naprakészek legyenek.