2024/2981

2024.12.4.

A BIZOTTSÁG (EU) 2024/2981 VÉGREHAJTÁSI RENDELETE

(2024. november 28.)

a 910/2014/EU európai parlamenti és tanácsi rendeletnek az európai digitális személyiadat-tárcák tanúsítása 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 5c. cikke (6) bekezdésére,

mivel:

(1) A 910/2014/EU rendelet 5c. cikke értelmében az európai digitális személyiadat-tárcák (a továbbiakban: adattárcák) tanúsítását nagy fokú biztonságuk és megbízhatóságuk biztosítása érdekében funkcionális, kiberbiztonsági és adatvédelmi követelményekkel összhangban kell elvégezni. Ezeket a tanúsítási követelményeket harmonizálni kell a tagállamok között a piac széttagoltságának megelőzése és egy szilárd keret kialakítása érdekében.

(2) Az e rendelet szerinti személyesadat-kezelési tevékenységre az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([2]) és adott esetben a 2002/58/EK európai parlamenti és tanácsi irányelv ([3]) alkalmazandó.

(3) A Bizottság rendszeresen értékeli az új technológiákat, gyakorlatokat, szabványokat és technikai specifikációkat. Az adattárcák fejlesztése és tanúsítása terén a tagállamok közötti lehető legmagasabb szintű harmonizáció biztosítása érdekében az e rendeletben meghatározott technikai specifikációk az európai digitális személyazonossági keretre irányuló összehangolt megközelítés közös uniós eszköztáráról szóló, 2021. június 3-i (EU) 2021/946 bizottsági ajánlás ([4]) nyomán elvégzett munkára támaszkodnak, különösen a keret részét képező architektúra és referenciakeret tekintetében. Az (EU) 2024/1183 európai parlamenti és tanácsi rendelet ([5]) (75) preambulumbekezdése értelmében a Bizottságnak rendszeresen felül kell vizsgálnia, és szükség esetén aktualizálnia kell ezt a végrehajtási rendeletet, hogy az megfeleljen a globális fejleményeknek, az architektúrának és a referenciakeretnek, valamint igazodjon a belső piaci bevált gyakorlatokhoz.

(4) A tanúsítási keretben foglalt kiberbiztonsági követelményeknek való megfelelés tanúsítása érdekében az adattárca-megoldások tanúsítása során az (EU) 2019/881 európai parlamenti és tanácsi rendelet ([6]) alapján létrehozott európai kiberbiztonsági tanúsítási rendszerekre kell hivatkozni, amennyiben vannak ilyenek és relevánsak. Arra az esetre, ha nincsenek, vagy csak részben fedik le a kiberbiztonsági követelményeket, e rendelet meghatározza a nemzeti tanúsítási rendszerekre alkalmazandó általános követelményeket, amelyek funkcionális, kiberbiztonsági és adatvédelmi követelményeket foglalnak magukban.

([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) 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).
([3]) 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]) HL L 210., 2021.6.14., 51. o., ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) 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 Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) A 910/2014/EU rendelet 5a. cikke (11) bekezdésének értelmében az adattárcákat a 910/2014/EU rendeletben, valamint az (EU) 2015/1502 bizottsági végrehajtási rendeletben ([7]) meghatározott „magas” biztonsági szinten kell tanúsítani. Ezt a biztonsági szintet az általános adattárca-megoldásnak kell elérnie. E rendelet értelmében az adattárca-megoldás egyes összetevői alacsonyabb biztonsági szinten is tanúsíthatók, feltéve, hogy ez kellően indokolt, és nem sérül az általános megoldás által elért magas biztonsági szint.

(6) Valamennyi nemzeti tanúsítási rendszer keretében ki kell jelölni egy, a tanúsítási rendszer fejlesztéséért és karbantartásáért felelős rendszertulajdonost. A rendszertulajdonos lehet megfelelőségértékelő szervezet, kormányzati szerv vagy hatóság, szakmai szövetség, megfelelőségértékelő szervezetek csoportja vagy bármely más megfelelő szervezet, és nem kell megegyeznie a nemzeti tanúsítási rendszert működtető szervezettel.

(7) A tanúsítás tárgyának ki kell terjednie az adattárca-megoldás szoftverkomponenseire, például az adattárcapéldányra. Az adattárca-biztonsági kriptográfiai alkalmazásokat (WSCA), az adattárca-biztonsági kriptográfiai eszközt (WSCD) és azokat a platformokat, amelyeken ezeket a szoftverkomponenseket végrehajtják, a működési környezet részeként csak akkor lehet a tanúsítás tárgyává tenni, ha azokat az adattárca-megoldás szolgáltatja. Más esetekben és különösen akkor, ha ezeket az eszközöket és platformokat végfelhasználók biztosítják, a szolgáltatóknak feltételezéseket kell alkotniuk az adattárca-megoldás működési környezetét, köztük az említett eszközöket és platformokat illetően is, és intézkedéseket kell hozniuk, amelyekkel megerősítik, hogy e feltételezések gyakorlati ellenőrzése megtörténik. Annak érdekében, hogy a WSCD által létrehozott, tárolt vagy feldolgozott kriptográfiai kulcsok kezelésére és védelmére használt hardverek és rendszerszoftverek megfelelő védelmet nyújtsanak a kritikus eszközök számára, a WSCD-nek – az EAL4-es szintű értékelés és az AVA_VAN.5-höz hasonlóan fejlett módszertani sebezhetőségi elemzés alapján – olyan magas szintű tanúsítási előírásoknak kell megfelelnie, mint amilyeneket például az (EU) 2024/482 bizottsági végrehajtási rendelettel ([8]) megállapított, közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) mint nemzetközi szabvány tartalmaz. Ezeket a tanúsítási előírásokat legkésőbb akkor alkalmazni kell, amikor az (EU) 2019/881 rendelet alapján elfogadott európai kiberbiztonsági tanúsítási rendszer szerint sor kerül az adattárcák megfelelőségének tanúsítására.

(8) A teljes mértékben mobil, biztonságos és felhasználóbarát adattárcákat illetéktelen módosítás ellen védett, szabványosított és tanúsított megoldások támogatják, például beágyazott biztonságos elemek, illetve olyan külső eszközök, mint az intelligens kártyák vagy mobil eszközökbe beépített SIM-platformok. Fontos, hogy időben rendelkezésre álljanak a nemzeti elektronikus személyazonosítási eszközökhöz és adattárcákhoz kialakított, beágyazott biztonsági elemek, és a tagállamok e területen tett erőfeszítéseit össze kell hangolni. A 910/2014/EU rendelet 46e. cikkének (1) bekezdése alapján létrehozott, az európai digitális személyazonossággal foglalkozó együttműködési csoportnak (a továbbiakban: együttműködési csoport) ezért erre a célra külön alcsoportot kell létrehoznia. Az érintett érdekelt felekkel konzultálva ennek az alcsoportnak meg kell állapodnia egy közös ütemtervről, amely a beágyazott biztonságos elemekhez való hozzáférés biztosítására irányul; ezt az ütemtervet a Bizottságnak figyelembe kell vennie a 910/2014/EU rendeletről szóló felülvizsgálati jelentés elkészítésekor. Az adattárca nemzeti szintű használatának előmozdítása érdekében a Bizottságnak továbbá a tagállamokkal együttműködve az architektúra és a referenciakeret részeként kézikönyvet kell kidolgoznia, amelyet folyamatosan naprakészen kell tartania a felhasználási esetek tekintetében.

(9) A nemzeti tanúsítási rendszerek keretében végzett tanúsítás tárgyának ki kell terjednie az adattárca-megoldás rendelkezésre bocsátására és működtetésére használt folyamatokra is, még akkor is, ha ezen eljárások meghatározását vagy végrehajtását harmadik feleknek alvállalkozásba adják. Annak igazolására, hogy a folyamatok megfelelnek a rendszerek követelményeinek, megbízhatósági információk is használhatók bizonyítékként, feltéve, hogy azok elégséges voltát függőségi elemzés alapján állapítják meg. A megbízhatósági információk számos különböző formát ölthetnek, többek között lehetnek jelentések és megfelelőségi tanúsítványok, amelyek lehetnek magántanúsítványok, illetve nemzeti, európai vagy nemzetközi szintűek, alapulhatnak szabványokon vagy technikai specifikációkon. A függőségi elemzés célja az adattárca összetevőiről rendelkezésre álló megbízhatósági információk minőségének értékelése.

([7]) A Bizottság (EU) 2015/1502 végrehajtási rendelete (2015. szeptember 8.) az elektronikus azonosító eszközök biztonsági szintjeire vonatkozó minimális technikai specifikációknak és eljárásoknak a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 8. cikkének (3) bekezdése szerint történő megállapításáról (HL L 235., 2015.9.9., 7. o., ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) 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/2024/482/oj).

(10) Az idevágó eljárásokat követve az együttműködési csoport számára lehetővé kell tenni, hogy véleményeket és ajánlásokat fogalmazzon meg a nemzeti tanúsítási rendszerek elé terjesztett tervezeteiről. Ezeknek a nemzeti tanúsítási rendszereknek kifejezetten az adattárca-architektúrára kell vonatkozniuk, és minden egyes támogatott architektúrához külön profilt kell rendelniük.

(11) Az adattárcák rendelkezésre bocsátását és működtetését esetlegesen érintő legkritikusabb kockázatok értékelésének egységes értelmezése és harmonizált megközelítése érdekében össze kell állítani egy nyilvántartást a kockázatokról és veszélyforrásokról, amelyet az adattárca-megoldások kialakításakor azok sajátos architektúrájától függetlenül figyelembe kell venni. Annak meghatározásakor, hogy mely kockázatokat kell felvenni a nyilvántartásba, szem előtt kell tartani a 910/2014/EU rendeletben ismertetett kiberbiztonsági célkitűzéseket, például az adattárca-megoldás titkosítását, integritását és rendelkezésre állását, valamint a felhasználók magánéletének védelmét és az adatvédelmet. Az ebben a kockázat-nyilvántartásban szereplő kockázatok és veszélyforrások kellő mértékű figyelembevétele a nemzeti tanúsítási rendszerekben foglalt követelményeknek is részét kell, hogy képezze. A folyamatosan változó fenyegetettségi helyzettel való összhang érdekében a kockázat-nyilvántartást karban kell tartani és rendszeresen aktualizálni kell, közösen az együttműködési csoporttal.

(12) Tanúsítási rendszereik kialakításakor a rendszertulajdonosoknak kockázatértékelést kell végezniük, hogy pontosabban meghatározzák a nyilvántartásban felsorolt kockázatokat és veszélyforrásokat, és kiegészítsék az adattárca-megoldás architektúrájához vagy megvalósításához kapcsolódó specifikus kockázatokkal és veszélyforrásokkal. A kockázatértékelésben figyelembe kell venni az ilyen kockázatok és veszélyforrások legmegfelelőbb kezelési módját. Az adattárca-szolgáltatóknak pedig az adattárca megvalósítására jellemző kockázatok és veszélyforrások azonosításával kell kiegészíteniük a rendszer kockázatértékelését, és ezek kezelésére megfelelő intézkedéseket kell javasolniuk, amelyeket a tanúsító szervnek értékelnie kell.

(13) Annak bizonyítása érdekében, hogy az adattárca-megoldás architektúrája megfelel az alkalmazandó biztonsági követelményeknek, minden egyes architektúraspecifikus rendszernek vagy profilnak tartalmaznia kell legalább a következőket: az adattárca-megoldás architektúrájának leírása, az adattárca-megoldás architektúrájára vonatkozó biztonsági követelmények felsorolása, egy annak megerősítésére irányuló értékelés terve, hogy az ezen architektúrán alapuló adattárca-megoldás megfelel az említett követelményeknek, valamint egy kockázatértékelés. A nemzeti tanúsítási rendszereknek elő kell írniuk az adattárca-szolgáltatók számára annak bizonyítását, hogy az általuk nyújtott adattárca-megoldás kialakítása miként feleltethető meg a referenciaarchitektúrának, valamint azt is, hogy részletesen ismertessék az adott adattárca-megoldásra vonatkozó biztonsági ellenőrzéseket és érvényesítési terveket. A nemzeti tanúsítási rendszereknek megfelelőségértékelési tevékenységet is meg kell határozniuk, amellyel ellenőrizhető, hogy az adattárca kialakítása jól tükrözi-e a kiválasztott profil referenciaarchitektúráját. A nemzeti tanúsítási rendszereknek meg kell felelniük az (EU) 2019/881 rendelet 51. cikkében meghatározott követelményeknek, az adatnaplózással kapcsolatos e) és f) pont kivételével.

(14) A termékek tanúsításának céljára meg kell engedni az EUCC keretében kibocsátott megfelelőségi tanúsítványok és a SOG-IS kölcsönös elismerési megállapodás alapján a nemzeti tanúsítási rendszerek keretében kibocsátott megfelelőségi tanúsítványok használatát. Ezenkívül lehetővé kell tenni más nemzeti tanúsítási rendszerek használatát is a kevésbé érzékeny termékösszetevők esetében, például a rögzített idejű kiberbiztonsági értékelési módszertanra vonatkozó CEN EN 17640 szabvány szerint létrehozott rendszerek esetében.

(15) Annak egyértelmű, egyszerű és felismerhető módon történő jelzésére, hogy az adattárcát a 910/2014/EU rendelettel összhangban bocsátották rendelkezésre, az európai digitális személyiadat-tárca bizalmi jegyét (a továbbiakban: bizalmi jegy) kell használni. Ezt tehát a nemzeti tanúsítási rendszerek keretében tanúsított adattárca-megoldások megfelelőségi jelölésének kell tekinteni. A nemzeti tanúsítási rendszerek más megfelelőségi jelet nem határozhatnak meg.

(16) A csalás visszaszorítása érdekében a nemzeti tanúsítási rendszereknek intézkedéseket kell meghatározniuk arra az esetre, ha valaki csalárd módon állítja, hogy rendelkezik a rendszer szerinti tanúsítással.

(17) A sebezhetőségi bejelentések hatékony kezelésének biztosítása érdekében az adattárca-megoldások és a megoldások szolgáltatására használt elektronikus azonosítási rendszer szolgáltatóinak folyamatokat kell meghatározniuk és végrehajtaniuk a sebezhetőségek súlyosságának és lehetséges hatásának értékelésére. A nemzeti tanúsítási rendszereknek meg kell határozniuk azt a küszöbértéket, amelynek meghaladásakor bejelentést kell küldeni a tanúsító szervnek. Ez a bejelentési kötelezettség nem érintheti az adatvédelmi incidensek bejelentésére vonatkozóan az adatvédelmi jogszabályok és a tagállamok adatvédelmi hatóságai által megállapított kritériumokat. Az adattárca-megoldások megsértésének vagy veszélyeztetésének kötelező bejelentése és az adatvédelmi incidenseknek az (EU) 2016/679 rendelet szerinti bejelentése között szinergiák lehetségesek, amelyeket fel kell feltárni. A sebezhetőségi hatásvizsgálati jelentés tanúsító szerv általi értékelése nem érintheti az adatvédelmi hatóságnak az (EU) 2016/679 rendelet 35. és 36. cikke szerinti adatvédelmi hatásvizsgálatra vonatkozó értékelését.

(18) Az adattárca-megoldások és a megoldások szolgáltatására használt elektronikus azonosítási rendszer szolgáltatóinak be kell jelenteniük a rendszertulajdonosnak minden olyan esetet, amikor indokolt a IV. mellékletben meghatározott, a WSCD és a WSCA értékeléséhez szükséges sebezhetőségi értékelés alóli felmentés.

(19) A megfelelőségi tanúsítvány törlése súlyos következményekkel járhat, mint például az összes telepített adattárcaegység érvénytelenítése. Ezért a tanúsító szervek csak akkor vehetik fontolóra a törlést, ha egy sebezhetőség orvoslás nélkül maradt, és így jelentősen befolyásolja a szóban forgó adattárca-megoldás vagy egy másik adattárca-megoldás megbízhatóságát.

(20) A nemzeti tanúsítási rendszerek aktualizálására külön eljárást kell bevezetni a rendszerek egymást követő verzióira való átállás kezelése érdekében, különösen a tekintetben, hogy a tanúsítvány jogosultjának milyen lépéseket kell tennie a soron következő értékelésekkel, valamint a karbantartási, az újratanúsítási és a különleges értékelésekkel kapcsolatban.

(21) Az átláthatóság érdekében az adattárca-szolgáltatóknak nyilvánosan meg kell osztaniuk az adattárca-megoldásukra vonatkozó biztonsági információkat.

(22) Amennyiben a nemzeti tanúsítási rendszerek más tanúsítási rendszerekből vagy forrásokból származó megbízhatósági információkra támaszkodnak, függőségi elemzést kell végezni annak ellenőrzésére, hogy a megbízhatósági dokumentáció – például megbízhatósági jelentések és megfelelőségi tanúsítványok – rendelkezésre áll-e, és megfelelő-e az adattárca-megoldások és a megoldások szolgáltatására használt elektronikus azonosítási rendszer szempontjából. A függőségi elemzés alapját az adattárca-megoldások és a megoldások szolgáltatására használt elektronikus azonosítási rendszer kockázatértékelésének kell képeznie. Az értékelésnek meg kell határoznia, hogy az adattárca-megoldás és a megoldás szolgáltatására használt elektronikus azonosítási rendszer tekintetében rendelkezésre álló megbízhatósági dokumentáció megfelelő-e a célzott értékelési szintnek megfelelő megbízhatóság nyújtására. Az értékelésnek egyúttal aktualizálnia vagy szükség esetén teljes mértékben újra kell értékelnie a függőségi elemzést.

(23) A tanúsító szerveknek a megfelelőségi tanúsítványokat a nemzeti tanúsítási rendszerek keretében a 910/2014/EU rendelet 5d. cikke (2) bekezdésének a) pontjában említett, nyilvánosan hozzáférhető tanúsítási jelentéssel együtt kell kibocsátaniuk. A tanúsításra vonatkozó értékelő jelentést az együttműködési csoport rendelkezésére kell bocsátani.

(24) A nemzeti tanúsítási rendszereknek éves felügyeleti értékelést kell beütemezniük annak biztosítására, hogy az adattárcák kezelésével és karbantartásával kapcsolatos folyamatok hatékonyan működjenek, tehát úgy, ahogyan azt a folyamatokat meghatározó szakpolitikai rendelkezések előírják. A kétévente végzett sebezhetőségi értékelés a 910/2014/EU rendeletből eredő követelmény, amely azt hivatott biztosítani, hogy az adattárca-megoldás továbbra is megfelelően lefedi a kockázat-nyilvántartásban azonosított kiberbiztonsági kockázatokat és veszélyforrásokat, beleértve a fenyegetettségi helyzet mindenkori alakulását is. A „felügyeleti értékelések”, az „újratanúsítási értékelések” és a „különleges értékelések” fogalmának összhangban kell lennie az EN ISO/IEC 17021–1:2015 szabvánnyal.

(25) A tanúsítási ciklus a megfelelőségi tanúsítvány lejártával vagy egy sikeres újratanúsítási értékelést követően kibocsátott új megfelelőségi tanúsítvánnyal ér véget. Az újratanúsítási értékelésnek magában kell foglalnia a tanúsítás tárgyát képező valamennyi összetevő értékelését, beleértve a hatékonysági értékelést és adott esetben a sebezhetőségi értékelést is. Az újratanúsítás során lehetővé kell tenni az azon összetevőkre vonatkozó korábbi értékelések eredményeinek újbóli használátát, amelyek nem változtak.

(26) Amennyiben egy európai kiberbiztonsági tanúsítási rendszer elfogadására kerül sor, az azonos alkalmazási körű nemzeti tanúsítási rendszereknek az (EU) 2019/881 rendelet 57. cikkének (1) bekezdésében meghatározott átmeneti időszakot követően be kell szüntetniük a tanúsítványok kibocsátását.

(27) A harmonizáció és az interoperabilitás biztosítása érdekében a nemzeti tanúsítási rendszereknek a meglévő keretekre kell támaszkodniuk, és adott esetben a már benyújtott bizonyítékokat újból fel kell használniuk. A tagállamok megállapodásokat köthetnek a tanúsítási rendszerek vagy azok részeinek határokon átnyúló újbóli használatáról. Az Európai Bizottságnak és az ENISA-nak az együttműködési csoporttal támogatnia kell a tagállamokat nemzeti tanúsítási rendszereik kidolgozásában és karbantartásában, gondoskodva a tudásmegosztásról és a bevált gyakorlatok cseréjéről.

(28) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([9]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor az európai adatvédelmi biztossal, aki 2024. szeptember 30-án véleményt nyilvánított.

(29) Az e rendeletben meghatározott intézkedések összhangban vannak a 910/2014/EU rendelet 48. cikkének (1) bekezdésében említett bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy és hatály

Ez a rendelet referenciaszabványokat, valamint specifikációkat és eljárásokat állapít meg egy adattárca-tanúsításra szolgáló szilárd keret kiépítéséhez, amelyet rendszeresen aktualizálni kell annak érdekében, hogy az lépést tartson mind a technológia és a szabványok fejlődésével, mind az európai digitális személyazonossági keretre irányuló összehangolt megközelítés közös uniós eszköztáráról szóló (EU) 2021/946 ajánlás nyomán elvégzett munkával, különösen az architektúrát és a referenciakeretet illetően.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „adattárca-megoldás”: szoftverek, hardverek, szolgáltatások, beállítások és konfigurációk kombinációja, beleértve az adattárcapéldányokat, egy vagy több adattárca-biztonsági kriptográfiai alkalmazást és egy vagy több adattárca-biztonsági kriptográfiai eszközt;

2. „rendszertulajdonos”: egy tanúsítási rendszer kidolgozásáért és karbantartásáért felelős szervezet;

3. „a tanúsítás tárgya”: olyan termékek, folyamatok és szolgáltatások, illetve ezek kombinációja, amelyekre meghatározott követelmények vonatkoznak;

4. „adattárca-biztonsági kriptográfiai alkalmazás”: olyan alkalmazás, amely kritikus eszközöket kezel az adattárca-biztonsági kriptográfiai eszközhöz kapcsolódva és az eszköz kriptográfiai és nem kriptográfiai funkcióinak használatával;

5. „adattárcapéldány”: az adattárca-felhasználó eszközére vagy környezetére telepített és konfigurált alkalmazás, amely egy adattárcaegység részét képezi, és amelyet az adattárca-felhasználó az adattárcaegységgel folytatott interakcióhoz használ;

([9]) 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).

6. „adattárca-biztonsági kriptográfiai eszköz”: olyan, illetéktelen módosítás ellen védett eszköz, amely egy, az adattárca-biztonsági kriptográfiai alkalmazáshoz kapcsolódó és általa használt környezetet biztosít a kritikus eszközök védelme és a kritikus műveletek biztonságos végrehajtásához szükséges kriptográfiai funkciók biztosítása érdekében;

7. „kockázat-nyilvántartás”: az azonosított kockázatokkal kapcsolatos, a tanúsítási eljárás szempontjából releváns információk nyilvántartása;

8. „adattárca-szolgáltató”: adattárca-megoldásokat kínáló természetes vagy jogi személy;

9. „tanúsító szerv”: harmadik félnek minősülő megfelelőségértékelő szervezet, amely tanúsítási rendszereket működtet;

10. „adattárcaegység”: az adattárca-megoldás egyedi konfigurációja, amely olyan adattárcapéldányokat, adattárca-biztonsági kriptográfiai alkalmazásokat és adattárca-biztonsági kriptográfiai eszközöket foglal magában, amelyeket az adattárca-szolgáltató nyújt egy adott adattárca-felhasználónak;

11. „kritikus eszközök”: az adattárcaegységen belüli vagy azzal kapcsolatban álló olyan rendkívüli jelentőségű adatok, eszközök, amelyek rendelkezésre állásának, titkosításának és integritásának sérülése nagyon súlyosan károsítaná az adattárcaegység megbízhatóságát;

12. „adattárca-felhasználó”: az a felhasználó, aki az adattárcaegység felett ellenőrzést és irányítást gyakorol;

13. „biztonsági esemény”: az (EU) 2022/2555 európai parlamenti és tanácsi irányelv ([10]) 6. cikkének 6. pontjában meghatározott biztonsági esemény;

14. „beágyazott közzétételi szabályzat”: a szolgáltató által elektronikus attribútumtanúsítványba ágyazva közzétett szabályrendszer, amely leírja, hogy mely feltételeknek kell eleget tennie az adattárca-igénybevevőnek az elektronikus attribútumtanúsítványhoz való hozzáféréshez.

II. FEJEZET

NEMZETI TANÚSÍTÁSI RENDSZEREK

3. cikk

A nemzeti tanúsítási rendszerek létrehozása

(1) A tagállamok minden nemzeti tanúsítási rendszerhez rendszertulajdonost jelölnek ki.

(2) A tanúsítás nemzeti tanúsítási rendszerekben meghatározott tárgya az adattárca-megoldások és a megoldások szolgáltatására használt elektronikus azonosítási rendszer rendelkezésre bocsátása és működtetése.

(3) Az (EU) 2015/1502 végrehajtási rendelettel összhangban a nemzeti tanúsítási rendszerekben a tanúsítás tárgya a következő elemekre terjed ki:

a) a szoftverkomponensek, beleértve az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszer beállításait és konfigurációit;

b) azon hardverkomponensek és -platformok, amelyeken a b) pontban említett szoftverkomponensek a kritikus műveletek során futnak, vagy amelyekre támaszkodnak, azokban az esetekben, amikor azokat közvetlenül vagy közvetve az adattárca-megoldás és a megoldás szolgáltatására használt elektronikus azonosítási rendszer biztosítja, és amennyiben azoknak e szoftverkomponensek tekintetében meg kell felelniük a kívánt biztonsági szintnek. Amennyiben a hardverkomponenseket és -platformokat nem az adattárca-szolgáltató nyújtja, a nemzeti tanúsítási rendszerek a hardverkomponensek és -platformok értékeléséhez feltételezéseket fogalmaznak meg, amelyek alapján az (EU) 2015/1502 végrehajtási rendelettel összhangban biztosítható a nagy támadási potenciálú támadókkal szembeni ellenállás, és meghatározzák az e feltételezések megerősítésére irányuló értékelési tevékenységeket, amelyeket a IV. melléklet említ;

([10]) Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (HL L 333., 2022.12.27., 80. o., ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) az adattárca-megoldás rendelkezésre bocsátását és működtetését támogató folyamatok, köztük a 910/2014/EU rendelet 5a. cikkében említett felhasználói beléptetési eljárás, amely legalább az (EU) 2015/1502 végrehajtási rendelet I. mellékletének 2.1., 2.2. és 2.4. szakasza szerinti nyilvántartásba vételt, az elektronikus eszközök irányítását, illetve a szervezést magában foglalja.

(4) A nemzeti tanúsítási rendszerek tartalmazzák az adattárca-megoldások és a megoldások szolgáltatására használt elektronikus azonosítási rendszer sajátos architektúrájának leírását. Amennyiben a nemzeti tanúsítási rendszerek több konkrét architektúrát is lefednek, minden egyes architektúrához külön profilt rendelnek.

(5) A nemzeti tanúsítási rendszerek minden profil esetében meghatározzák legalább a következőket:

a) az adattárca-megoldás és a megoldás szolgáltatására használt elektronikus azonosítási rendszer konkrét architektúrája;

b) a 910/2014/EU rendelet 8. cikkében meghatározott biztonsági szintekhez kapcsolódó biztonsági ellenőrzések;

c) az EN ISO/IEC 17065/2012 szabvány 7.4.1. pontjával összhangban elkészített értékelési terv;

d) az e rendelet I. mellékletében meghatározott kockázat-nyilvántartásban felsorolt kiberbiztonsági kockázatok és veszélyforrások kezeléséhez szükséges biztonsági követelmények az előírt biztonsági szintig, valamint adott esetben az (EU) 2019/881 rendelet 51. cikkében meghatározott célkitűzések teljesítéséhez;

e) az e bekezdés b) pontjában említett ellenőrzések hozzárendelése az architektúra összetevőihez;

f) annak leírása, hogy a b)–c) pontban említett biztonsági ellenőrzések, a hozzárendelésük, a biztonsági követelmények és értékelési terv hogyan teszik lehetővé az adattárca-megoldások és a megoldás szolgáltatására használt elektronikus azonosítási rendszer szolgáltatói számára, hogy az előírt biztonsági szintig megfelelően kezeljék a d) pontban említett kockázat-nyilvántartásban azonosított kiberbiztonsági kockázatokat és veszélyforrásokat, azon kockázatértékelés alapján, amelynek célja a kockázat-nyilvántartásban felsorolt kockázatok és veszélyforrások pontosabb meghatározása és annak az architektúrára jellemző kockázatokkal és veszélyforrásokkal való kiegészítése.

(6) Az (5) bekezdés c) pontjában említett értékelési terv felsorolja azokat az értékelési tevékenységeket, amelyeket az adattárca-megoldások és a megoldások szolgáltatására használt elektronikus azonosítási rendszer értékelésének magában kell foglalnia.

(7) A (6) bekezdésben említett értékelési tevékenységek keretében az adattárca-megoldások és a megoldás szolgáltatására használt elektronikus azonosítási rendszer szolgáltatói kötelesek olyan információkat szolgáltatni, amelyek megfelelnek a II. mellékletben felsorolt követelményeknek.

4. cikk

Általános követelmények

(1) A nemzeti tanúsítási rendszerek funkcionális, kiberbiztonsági és adatvédelmi követelményeket is magukban foglalnak a következő tanúsítási rendszerekre hagyatkozva, amennyiben ezek rendelkezésre állnak és alkalmazandók:

a) az (EU) 2019/881 rendelet alapján létrehozott európai kiberbiztonsági tanúsítási rendszerek, beleértve az EUCC-t is;

b) az EUCC hatálya alá tartozó nemzeti kiberbiztonsági tanúsítási rendszerek, az (EU) 2024/482 végrehajtási rendelet 49. cikkével összhangban.

(2) A nemzeti tanúsítási rendszerek emellett – amennyiben rendelkezésre állnak és alkalmazandók – hivatkozhatnak a következőkre:

a) egyéb nemzeti tanúsítási rendszerek;

b) nemzetközi, európai és nemzeti szabványok;

c) az 1025/2012/EU európai parlamenti és tanácsi rendelet ([11]) II. mellékletében meghatározott követelményeknek megfelelő műszaki előírások.

(3) A nemzeti tanúsítási rendszerek:

a) meghatározzák az EN ISO/IEC 17067:2013 szabvány 6.5. pontjában felsorolt elemeket;

b) az EN ISO/IEC 17067:2013 szabvány 5.3.8. pontjával összhangban 6-os típusú rendszerként kerülnek végrehajtásra.

(4) A nemzeti tanúsítási rendszerek megfelelnek a következő követelményeknek:

a) kizárólag a 910/2014/EU rendelet 5a. cikkének (2) bekezdésében említett szolgáltatók jogosultak tanúsítványok nemzeti tanúsítási rendszerek keretében történő kibocsátására;

b) megfelelőségi jelölésként csak a bizalmi jegyet használják;

c) az adattárca-megoldások és a megoldásokat szolgáltató elektronikus azonosítási rendszer szolgáltatói a rendszerre való hivatkozáskor a 910/2014/EU rendeletre és erre a rendeletre hivatkoznak;

d) az adattárca-megoldások és a megoldásokat szolgáltató elektronikus azonosítási rendszer szolgáltatói kiegészítik a rendszernek a 3. cikk (5) bekezdése f) pontjában említett kockázatértékelését annak érdekében, hogy azonosítsák az adattárca-megoldások megvalósításához kapcsolódó kockázatokat és veszélyforrásokat, és megfelelő intézkedéseket javasoljanak valamennyi releváns kockázat és veszélyforrás kezelésére;

e) megállapítják a felelősségi köröket és a jogi lépéseket, és hivatkoznak a felelősségi köröket és az akkor alkalmazandó lehetséges jogi lépéseket tartalmazó nemzeti jogszabályokra, amennyiben a rendszer szerinti tanúsítást csalárd módon alkalmazzák.

(5) A (4) bekezdés d) pontjában említett kockázatértékelést meg kell osztani a tanúsító szervvel értékelés céljából.

5. cikk

A biztonsági események és a sebezhetőségek kezelése

(1) A nemzeti tanúsítási rendszerek a biztonsági események és sebezhetőségek kezelésére vonatkozó követelményeket tartalmaznak a (2)–(9) bekezdésnek megfelelően.

(2) Az adattárca-megoldásra és a megoldást szolgáltató elektronikus azonosítási rendszerre vonatkozó megfelelőségi tanúsítvány jogosultja indokolatlan késedelem nélkül bejelenti a megfelelő tanúsító szervnek az adattárca-megoldás vagy a megoldást szolgáltató elektronikus azonosítási rendszer megsértését vagy veszélyeztetését minden olyan esetben, ha az hatással lehet az adattárca-megoldás vagy az elektronikus azonosítási rendszer nemzeti tanúsítási rendszerek követelményeinek való megfelelésére.

(3) A megfelelőségi tanúsítvány jogosultja a sebezhetőségek kezelésére szabályzatot és eljárásokat dolgoz ki, tart fenn és működtet, figyelembe véve a meglévő európai és nemzetközi szabványokban, többek között az EN ISO/IEC 30111:2019 szabványban meghatározott eljárásokat.

(4) A megfelelőségi tanúsítvány jogosultja bejelenti a kibocsátó tanúsító szervnek azokat a sebezhetőségeket és változásokat, amelyek az adattárca-megoldást érintik, az e sebezhetőségek és változások hatására vonatkozó meghatározott kritériumok alapján.

(5) A megfelelőségi tanúsítvány jogosultja sebezhetőségi hatásvizsgálati jelentést készít minden olyan sebezhetőségről, amely az adattárca-megoldás szoftverkomponenseit érinti. A jelentés tartalmazza a következő információkat:

a) a tanúsított adattárca-megoldás sebezhetőségének hatása;

b) a támadás közelségével vagy valószínűségével kapcsolatos lehetséges kockázatok;

([11]) Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről, EGT-vonatkozású szöveg (HL L 316., 2012.11.14., 12. o., ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) orvosolható-e a sebezhetőség a rendelkezésre álló eszközökkel;

d) amennyiben a sebezhetőség orvosolható a rendelkezésre álló eszközökkel, a sebezhetőség orvoslásának lehetséges módjai.

(6) Amennyiben a (4) bekezdés szerinti bejelentésre van szükség, a megfelelőségi tanúsítvány jogosultja indokolatlan késedelem nélkül továbbítja az (5) bekezdésben említett sebezhetőségi hatásvizsgálati jelentést a tanúsító szervnek.

(7) A megfelelőségi tanúsítvány jogosultja a sebezhetőségek kezelésére a kiberrezilienciáról szóló jogszabály ([12]) I. mellékletében meghatározott követelményeknek megfelelő szabályzatot dolgoz ki, tart fenn és működtet.

(8) A nemzeti tanúsítási rendszerek meghatározzák a tanúsítási szervekre alkalmazandó sebezhetőségfeltárási követelményeket.

(9) A megfelelőségi tanúsítvány jogosultja köteles az adattárca-megoldás minden nyilvánosan ismert és orvosolt sebezhetőségét az V. mellékletben említett online adattárak valamelyikében közzétenni és nyilvántartásba venni.

6. cikk

A nemzeti tanúsítási rendszerek karbantartása

(1) A nemzeti tanúsítási rendszerek eljárást tartalmaznak működésük rendszeres időközönkénti felülvizsgálatára. Ezen eljárás célja a rendszerek megfelelőségének megerősítése és a javításra szoruló szempontok azonosítása, figyelembe véve az érdekelt felek visszajelzéseit.

(2) A nemzeti tanúsítási rendszerek a karbantartásukra vonatkozó rendelkezéseket is tartalmaznak. Az említett eljárás legalább a következő követelményeket foglalja magában:

a) a nemzeti tanúsítási rendszerek meghatározásának és követelményeinek irányítására vonatkozó szabályok;

b) a tanúsítványok kibocsátására vonatkozó határidők megállapítása a nemzeti tanúsítási rendszerek aktualizált verzióinak elfogadását követően, mind az új, mind a korábban kibocsátott megfelelőségi tanúsítványok esetében;

c) a nemzeti tanúsítási rendszerek rendszeres felülvizsgálata annak biztosítása érdekében, hogy az azokban megállapított követelményeket következetesen alkalmazzák, figyelembe véve legalább a következő szempontokat:

— a nemzeti tanúsítási rendszer követelményeivel kapcsolatban a rendszertulajdonoshoz intézett, pontosításra irányuló kérések,

— az érdekelt felektől és más érintettektől kapott visszajelzések,

— a nemzeti tanúsítási rendszer tulajdonosának információkérésekre való reagálókészsége;

d) a referenciadokumentumok nyomon követésére vonatkozó szabályok és a nemzeti tanúsítási rendszerek referencia-verzióinak alakulására vonatkozó eljárások, legalább az átmeneti időszakok tekintetében;

e) egy folyamat annak biztosítására, hogy az e rendelet I. mellékletében meghatározott kockázat-nyilvántartásban felsorolt legújabb kiberbiztonsági kockázatok és veszélyforrások le legyenek fedve;

f) a nemzeti tanúsítási rendszerek egyéb változásainak kezelésére szolgáló folyamat.

([12]) Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet) (HL L, 2024/2847, 2024.11.20., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(3) A nemzeti tanúsítási rendszerek követelményeket tartalmaznak az aktuálisan tanúsított termékek értékelésére, amelyet a rendszer felülvizsgálatát követő bizonyos időszakon belül vagy az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszer által teljesítendő új specifikációk vagy szabványok vagy azok új verzióinak közzétételét követően kell elvégezni.

III. FEJEZET

A RENDSZERTULAJDONOSOKRA VONATKOZÓ KÖVETELMÉNYEK

7. cikk

Általános követelmények

(1) A rendszertulajdonosok nemzeti tanúsítási rendszereket dolgoznak ki és tartanak karban, és szabályozzák működésüket.

(2) A rendszertulajdonosok feladataikat teljesen vagy részben alvállalkozásba adhatják harmadik félnek. Magánfélnek történő alvállalkozásba adáskor a rendszertulajdonosok szerződésben határozzák meg valamennyi fél kötelezettségeit és felelősségi körét. Az alvállalkozóik által végzett valamennyi alvállalkozói tevékenységért továbbra is a rendszertulajdonosok felelnek.

(3) A rendszertulajdonosok nyomonkövetési tevékenységük során adott esetben legalább a következő információkat figyelembe veszik:

a) a tanúsító szervektől, a nemzeti akkreditáló testületektől és az érintett piacfelügyeleti hatóságoktól származó információk;

b) a saját vagy más hatóság által végzett ellenőrzésekből és vizsgálatokból származó információk;

c) a 15. cikk alapján beérkezett panaszok és jogorvoslat iránti kérelmek.

(4) A rendszertulajdonosok tájékoztatják az együttműködési csoportot, ha a nemzeti tanúsítási rendszerek felülvizsgálatára kerül sor. Az értesítésben megfelelő tájékoztatást kell nyújtani az együttműködési csoport számára ahhoz, hogy az ajánlásokat adjon ki a rendszertulajdonosoknak, és véleményt nyilvánítson az aktualizált nemzeti tanúsítási rendszerekről.

IV. FEJEZET

AZ ADATTÁRCA-MEGOLDÁSOK ÉS AZ AZOK BIZTOSÍTÁSÁRA HASZNÁLT ELEKTRONIKUS AZONOSÍTÁSI RENDSZER SZOLGÁLTATÓIRA VONATKOZÓ KÖVETELMÉNYEK

8. cikk

Általános követelmények

(1) A nemzeti tanúsítási rendszerek kiberbiztonsági követelményeket tartalmaznak minden egyes támogatott architektúra kockázatértékelése alapján. E kiberbiztonsági követelmények célja az I. mellékletben megállapított kockázatnyilvántartásban azonosított kiberbiztonsági kockázatok és veszélyforrások kezelése.

(2) A 910/2014/EU rendelet 5a. cikkének (23) bekezdésével összhangban a nemzeti tanúsítási rendszerek előírják, hogy az adattárca-megoldások és a megoldások szolgáltatására használt elektronikus azonosítási rendszerek az (EU) 2015/1502 végrehajtási rendeletben említett „magas” biztonsági szinten ellenállóak legyenek a nagy támadási potenciálú támadókkal szemben.

(3) A nemzeti tanúsítási rendszerek biztonsági kritériumokat állapítanak meg, amelyek a következő követelményeket foglalják magukban:

a) adott esetben a kiberrezilienciáról szóló jogszabályban meghatározott követelmények vagy az (EU) 2019/881 rendelet 51. cikkében meghatározott biztonsági célkitűzéseket teljesítő követelmények;

b) az adattárca-megoldás működtetésével kapcsolatos kockázatok kezelésére vonatkozó szakpolitikai intézkedések és eljárások kidolgozása és végrehajtása, beleértve a kockázatok azonosítását és értékelését, valamint az azonosított kockázatok mérséklését;

c) a változások kezelésére és a sebezhetőségek e rendelet 5. cikkével összhangban történő kezelésére vonatkozó szakpolitikai intézkedések és eljárások kidolgozása és végrehajtása;

d) humánerőforrás-gazdálkodási szakpolitikai intézkedések és eljárások kidolgozása és végrehajtása, beleértve az adattárca-megoldás kidolgozásában vagy működtetésében részt vevő személyzet szakértelmére, megbízhatóságára, tapasztalatára, biztonsági képzésére és képesítésére vonatkozó követelményeket;

e) az adattárca-megoldás működési környezetére vonatkozó követelmények, többek között feltételezések formájában azon eszközök és platformok biztonságára vonatkozóan, amelyeken az adattárca-megoldás szoftverkomponensei futnak, beleértve a WSCD-ket is, valamint adott esetben megfelelőségértékelési követelmények annak megerősítésére, hogy ezeket a feltételezéseket az érintett eszközökön és platformokon ellenőrzik;

f) minden olyan feltételezés esetében, amelyet nem támaszt alá megfelelőségi tanúsítvány vagy más elfogadható megbízhatósági információ, az adattárca-szolgáltató által a feltételezés megerősítésére használt mechanizmus leírása, valamint annak indoklása, hogy a mechanizmussal megfelelően ellenőrizhető a feltételezés;

g) az adattárca-megoldás aktuálisan tanúsított verziójának használatát biztosító intézkedések kidolgozása és végrehajtása.

(4) A nemzeti tanúsítási rendszerek funkcionális követelményeket tartalmaznak az adattárca-megoldások és a megoldások szolgáltatására használt elektronikus azonosítási rendszerek valamennyi szoftverkomponensére vonatkozó frissítési mechanizmusokra a III. mellékletben felsorolt műveletek tekintetében.

(5) A nemzeti tanúsítási rendszerek előírják, hogy a tanúsítás kérelmezője benyújtsa a tanúsító szervnek vagy más módon bocsássa annak rendelkezésére a következő információkat és dokumentációt:

a) a IV. melléklet 1. pontjában említett információkat alátámasztó bizonyítékok, szükség esetén az adattárca-megoldásra és forráskódjára vonatkozó részletek, beleértve a következőket:

— *az architektúrára vonatkozó információk:* az adattárca-megoldás minden egyes összetevője (beleértve a termék-, folyamat- és szolgáltatási összetevőket) esetében az alapvető biztonsági tulajdonságok leírása, beleértve a külső függőségeket is;

— *ellenőrzések és biztonsági szintek:* az adattárca-megoldás minden egyes biztonsági ellenőrzése esetében az ellenőrzés és a szükséges biztonsági szint leírása az (EU) 2015/1502 végrehajtási rendelet melléklete alapján, amely számos olyan technikai specifikációt és eljárást meghatároz, amely az elektronikus azonosító eszközök által végrehajtott különböző ellenőrzésekre alkalmazandó;

— *az ellenőrzések hozzárendelése az architektúra összetevőihez:* annak leírása, hogy az adattárca ellenőrzéseit hogyan hajtják végre az adattárca-megoldás különböző összetevőinek felhasználásával, megmagyarázva, hogy miért van szükség egy adott biztonsági szintre, és hogy miként hajtják végre az ellenőrzést az összes szükséges biztonsági szempont figyelembevételével a megfelelő szinten;

— *a kockázatok lefedésének magyarázata és indoklása:* a következők indoklása:

— az ellenőrzések hozzárendelése az összetevőkhöz,

— a javasolt értékelési terv alkalmas-e arra, hogy megfelelően lefedje az összes ellenőrzést,

— a kockázat-nyilvántartásban azonosított kiberbiztonsági kockázatok és veszélyforrások ellenőrzése által biztosított lefedettség, kiegészítve a végrehajtásra jellemző kockázatok és veszélyforrások megfelelő biztonsági szintű ellenőrzésével;

b) az V. mellékletben felsorolt információk;

c) az értékelési tevékenységek során bizonyítékként használt megfelelőségi tanúsítványok és egyéb megbízhatósági információk teljes listája;

d) az értékelési tevékenységek szempontjából releváns bármely egyéb információ.

V. FEJEZET

A TANÚSÍTÓ SZERVEKRE VONATKOZÓ KÖVETELMÉNYEK

9. cikk

Általános követelmények

(1) A tanúsító szerveket a 765/2008/EK európai parlamenti és tanácsi rendelet ([13]) szerint kijelölt nemzeti akkreditáló testületek akkreditálják az EN ISO/IEC 17065:2012 szabványnak megfelelően, amennyiben azok megfelelnek a nemzeti tanúsítási rendszerekben a (2) bekezdéssel összhangban meghatározott követelményeknek.

(2) Az akkreditációhoz a tanúsító szervek a kompetenciájukkal kapcsolatos összes alábbi követelményt teljesítik:

a) az adattárca-megoldás és a megoldás szolgáltatására használt elektronikus azonosítási rendszer releváns architektúráinak, valamint az ezen architektúrákhoz kapcsolódó veszélyforrásoknak és kockázatoknak a részletes és technikai ismerete;

b) a rendelkezésre álló biztonsági megoldások és azok tulajdonságainak ismerete az (EU) 2015/1502 végrehajtási rendelet mellékletének megfelelően;

c) az adattárca-megoldás és a megoldás szolgáltatására használt elektronikus azonosítási rendszer összetevőire irányuló, a megfelelőségi tanúsítványokkal kapcsolatban végzett tevékenységek ismerete, mivel azok tanúsítás tárgyát képezik;

d) a II. fejezettel összhangban létrehozott alkalmazandó nemzeti tanúsítási rendszer részletes ismerete.

(3) A tanúsító szervek felügyeleti tevékenységeiket különösen a következő információk alapján végzik:

a) a nemzeti akkreditáló testületektől és az érintett piacfelügyeleti hatóságoktól származó információk;

b) a saját vagy más hatóság által végzett ellenőrzésekből és vizsgálatokból származó információk;

c) a 15. cikk alapján beérkezett panaszok és jogorvoslat iránti kérelmek.

10. cikk

Alvállalkozás

A tanúsító szervek a 13. cikkben meghatározott értékelési tevékenységeket harmadik feleknek alvállalkozásba adhatják. Amennyiben az értékelési tevékenységeket alvállalkozásba adják, a nemzeti tanúsítási rendszerek megállapítják a következőket:

1. a tanúsító szerv értékelési tevékenységeket végző valamennyi alvállalkozója megfelel a vizsgálatok tekintetében az EN ISO/IEC 17025:2017, a helyszíni szemlék tekintetében az EN ISO/IEC 17020:2012, az ellenőrzések tekintetében az EN ISO/IEC 17021–1:2015, az érvényesítés és felülvizsgálat tekintetében pedig az EN ISO/IEC 17029:2019 harmonizált szabványok követelményeinek, amennyiben azok az elvégzendő tevékenységekre alkalmazandók és relevánsak;

2. a tanúsító szervek vállalják a felelősséget a más szerveknek kiszervezett valamennyi értékelési tevékenységért, és bizonyítják, hogy akkreditációjuk során megfelelő intézkedéseket hoztak, többek között adott esetben alvállalkozóik saját akkreditációjára támaszkodva;

3. a kiszervezéshez a rendszertulajdonosoktól vagy attól az ügyféltől beszerzendő előzetes hozzájárulás mértéke, akinek az adattárca-megoldását a tanúsítási rendszer keretében tanúsítják.

([13]) Az Európai Parlament és a Tanács 765/2008/EK rendelete (2008. július 9.) a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről (HL L 218., 2008.8.13., 30. o., ELI: http://data.europa.eu/eli/reg/2008/765/oj).

11. cikk

A felügyeleti szervnek küldött bejelentés

A tanúsító szervek bejelentik a 910/2014/EU rendelet 46a. cikkének (1) bekezdésében említett felügyeleti szervnek az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszer megfelelőségi tanúsítványainak kibocsátását, felfüggesztését és törlését.

12. cikk

A biztonsági események és a sebezhetőségek kezelése

(1) A tanúsító szervek indokolatlan késedelem nélkül felfüggesztik az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszer megfelelőségi tanúsítványát, miután megerősítették, hogy a biztonság bejelentett megsértése vagy veszélyeztetése hatással van arra, hogy az adattárca-megoldás és az annak biztosítására használt elektronikus azonosítási rendszer megfelel-e a nemzeti tanúsítási rendszerek követelményeinek.

(2) A tanúsító szervek törlik a biztonság megsértése vagy veszélyeztetése miatt felfüggesztett megfelelőségi tanúsítványokat, amennyiben a problémát nem orvosolják kellő időben.

(3) A tanúsító szervek a 910/2014/EU rendelet 5c. cikkének (4) bekezdésével és 5e. cikkének (2) bekezdésével összhangban törlik a megfelelőségi tanúsítványokat, ha az azonosított sebezhetőséget nem orvosolták kellő időben a súlyosságával és lehetséges hatásával arányosan.

VI. FEJEZET

MEGFELELŐSÉGÉRTÉKELÉSI TEVÉKENYSÉGEK

13. cikk

Értékelési tevékenységek

(1) A nemzeti tanúsítási rendszerek tartalmazzák a megfelelőségértékelő szervezetek által az EN ISO/IEC 17065:2012 szabványnak megfelelően végzett értékelési tevékenységeik során alkalmazandó módszereket és eljárásokat, amelyek legalább a következő szempontokra kiterjedek:

a) az értékelési tevékenységek elvégzésének módszerei és eljárásai, beleértve a WSCD-vel kapcsolatos tevékenységeket is a IV. mellékletben meghatározottak szerint;

b) az adattárca-megoldás és a megoldás szolgáltatására használt elektronikus azonosítási rendszer végrehajtásának ellenőrzése az I. mellékletben meghatározott kockázat-nyilvántartás alapján, szükség esetén a végrehajtásra jellemző kockázatokkal kiegészítve;

c) amennyiben rendelkezésre állnak és megfelelőek, technikai specifikációknak vagy szabványoknak megfelelően meghatározott vizsgálati sorozatokon alapuló funkcionális vizsgálati tevékenységek;

d) a karbantartási folyamatok meglétének és alkalmasságának értékelése, beleértve legalább a verziók, a frissítések és a sebezhetőségek kezelését;

e) a karbantartási folyamatok működési hatékonyságának értékelése, beleértve legalább a verziók, a frissítések és a sebezhetőségek kezelését;

f) az adattárca-szolgáltató által készített függőségi elemzés, beleértve a megbízhatósági információk elfogadhatóságának értékelésére szolgáló módszertant, amely tartalmazza a VI. mellékletben meghatározott elemeket;

g) a megfelelő szinten elvégzett sebezhetőségi értékelés, beleértve a következőket:

— az adattárca-megoldás kialakításának és adott esetben forráskódjának felülvizsgálata,

— az adattárca-megoldás nagy támadási potenciálú támadókkal szembeni ellenállásának vizsgálata „magas” biztonsági szinten az (EU) 2015/1502 végrehajtási rendelet mellékletének 2.2.1. szakasza szerint;

h) annak az értékelése, hogy miként alakul a fenyegetettségi környezet, és az milyen hatással van a kockázatok adattárca-megoldás általi lefedésére, annak meghatározása érdekében, hogy milyen értékelési tevékenységekre van szükség az adattárca-megoldás különböző összetevői tekintetében.

(2) A nemzeti tanúsítási rendszerek részét képezi egy értékelés annak megállapítására, hogy az adattárca-megoldások és az azok biztosítására használt elektronikus azonosítási rendszer végrehajtása összhangban van-e a 3. cikk (5) bekezdése a) pontjában meghatározott architektúrával, valamint egy értékelés annak megállapítására is, hogy a javasolt értékelési terv a végrehajtással együtt megfelel-e a 3. cikk (5) bekezdésének c) pontjában említett értékelési tervnek.

(3) A nemzeti tanúsítási rendszerek mintavételi szabályokat állapítanak meg annak érdekében, hogy ugyanazokra az értékelési tevékenységekre ne kerüljön sor többször is, és hogy a rendszer azokra a tevékenységekre összpontosítson, amelyek egy adott változatra jellemzőek. E mintavételi szabályoknak lehetővé kell tenniük, hogy a funkcionális és biztonsági vizsgálatokat csak az adattárca-megoldás és a megoldás szolgáltatására használt elektronikus azonosítási rendszer célkomponensének változataiból álló mintán, valamint a céleszközök mintáján végezzék el. A nemzeti tanúsítási rendszerek előírják minden tanúsító szerv számára, hogy indokolják az általuk alkalmazott mintavételt.

(4) A nemzeti tanúsítási rendszerek előírják, hogy a tanúsító szerv a IV. mellékletben meghatározott módszerek és eljárások alapján értékelje a WSCA-t.

14. cikk

Tanúsítási tevékenységek

(1) A nemzeti tanúsítási rendszerek tanúsítási tevékenységet határoznak meg az EN ISO/IEC 17067:2013 szabvány 1. táblázata V. szakaszának a) pontja szerinti megfelelőségi tanúsítvány kibocsátása céljából, a következő szempontokat figyelembe véve:

a) a megfelelőségi tanúsítvány VII. mellékletben meghatározott tartalma;

b) ahogyan jelenteni kell az értékelés eredményeit a nyilvános tanúsítási jelentésben, amelynek a VIII. mellékletben meghatározottak szerint legalább az előzetes ellenőrzési és érvényesítési terv összefoglalóját tartalmaznia kell;

c) a tanúsításra vonatkozó értékelő jelentésben szereplő értékelési eredmények tartalma, beleértve a VIII. mellékletben meghatározott elemeket is.

(2) A tanúsításra vonatkozó értékelő jelentés az együttműködési csoport és a Bizottság rendelkezésére bocsátható.

15. cikk

Panaszok és jogorvoslat iránti kérelmek

A nemzeti tanúsítási rendszerek eljárásokat vagy az alkalmazandó nemzeti jogszabályokra való hivatkozásokat tartalmaznak, amelyek meghatározzák a tanúsítási rendszer végrehajtásával vagy a kibocsátott megfelelőségi tanúsítvánnyal kapcsolatos panaszok és jogorvoslat iránti kérelmek hatékony benyújtására és kezelésére szolgáló mechanizmust. Ezen eljárások közé tartozik a panaszos tájékoztatása az eljárás előrehaladásáról és a meghozott határozatról, valamint arról, hogy joga van a hatékony bírósági jogorvoslathoz. A nemzeti tanúsítási rendszerek előírják, hogy minden olyan panaszt és jogorvoslat iránti kérelmet, amelyet a tanúsító szerv nem oldott meg, vagy nem tudott megoldani, értékelés és megoldás céljából továbbítsák a rendszertulajdonosnak.

16. cikk

Felügyeleti tevékenységek

(1) A nemzeti tanúsítási rendszerek előírják a tanúsító szervek számára, hogy olyan felügyeleti tevékenységeket hajtsanak végre, amelyek során a folyamatok felügyeleti értékelését véletlenszerű vizsgálatokkal vagy helyszíni szemlékkel kombinálják.

(2) A nemzeti tanúsítási rendszerek követelményeket tartalmaznak a rendszertulajdonosok számára annak nyomon követésére, hogy a tanúsító szervek teljesítik-e a 910/2014/EU rendelet és adott esetben a nemzeti tanúsítási rendszerek szerinti kötelezettségeiket.

(3) A nemzeti tanúsítási rendszerek követelményeket tartalmaznak a tanúsító szervek számára a következők nyomon követésére:

a) a nemzeti tanúsítási rendszerek keretében kibocsátott megfelelőségi tanúsítványok jogosultjai teljesítik-e a 910/2014/EU rendelet és a nemzeti tanúsítási rendszerek szerinti tanúsítási kötelezettségeiket;

b) a tanúsított adattárca-megoldás megfelel-e a nemzeti tanúsítási rendszerekben meghatározott követelményeknek.

17. cikk

A meg nem felelés következményei

A nemzeti tanúsítási rendszerek meghatározzák, hogy milyen következményekkel jár, ha a tanúsított adattárca-megoldás és a megoldás szolgáltatására használt elektronikus azonosítási rendszer nem felel meg az ebben a rendeletben meghatározott követelményeknek. E következmények az alábbi szempontokat foglalják magukban:

1. a tanúsító szervezet azon kötelezettsége, hogy tájékoztassa és felkérje a megfelelőségi tanúsítvány jogosultját korrekciós intézkedések alkalmazására;

2. a tanúsító szerv azon kötelezettsége, hogy tájékoztassa a többi érintett piacfelügyeleti hatóságot, amennyiben a meg nem felelés vonatkozó uniós jogszabályokat érint;

3. a megfelelőségi tanúsítvány jogosultja által végrehajtandó korrekciós intézkedések feltételei;

4. a megfelelőségi tanúsítvány tanúsító szerv általi felfüggesztésére és a megfelelőségi tanúsítványnak a meg nem felelés orvoslását követő helyreállítására vonatkozó feltételek;

5. a megfelelőségi tanúsítvány tanúsító szerv általi törlésének feltételei;

6. annak következményei, ha a tanúsító szerv nem felel meg a nemzeti tanúsítási rendszer követelményeinek.

VII. FEJEZET

A TANÚSÍTÁS ÉLETCIKLUSA

18. cikk

A tanúsítás életciklusa

(1) A nemzeti tanúsítási rendszerek keretében kibocsátott megfelelőségi tanúsítványok érvényességét a tanúsító szerv által a IX. mellékletben meghatározott követelményekkel összhangban végzett rendszeres értékelési tevékenységeknek kell alávetni.

(2) A nemzeti tanúsítási rendszerek egy folyamatot határoznak arra az esetre, ha a megfelelőségi tanúsítvány jogosultja az eredeti megfelelőségi tanúsítvány lejárta előtt az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszer újratanúsítását kéri. Ez az újratanúsítási folyamat magában foglalja az adattárca-megoldás és a megoldás szolgáltatására használt elektronikus azonosítási rendszer teljeskörű értékelését, beleértve a IX. mellékletben meghatározott elvek szerint elvégzett sebezhetőségi értékelést.

(3) A nemzeti tanúsítási rendszerek eljárást tartalmaznak a tanúsított adattárca-megoldásban és a megoldás szolgáltatására használt elektronikus azonosítási rendszerben bekövetkező változások kezelésére. Ennek az eljárásnak szabályokat kell tartalmaznia annak meghatározására, hogy egy adott változtatást a (4) bekezdésben említett különleges értékelésnek vagy a karbantartási folyamatok működési hatékonyságának a IV. mellékletben említett felülvizsgálatának kell-e alávetni.

(4) A nemzeti tanúsítási rendszerek magukban foglalják az EN ISO/IEC 17065:2012 szabvány szerinti különleges értékelések folyamatát. A különleges értékelések folyamata magában foglalja azon tevékenységek sorát, amelyeket a különleges értékelést kiváltó konkrét probléma kezelése érdekében el kell végezni.

(5) A nemzeti tanúsítási rendszerek meghatározzák a megfelelőségi tanúsítvány törlésére vonatkozó szabályokat.

VIII. FEJEZET

NYILVÁNTARTÁS ÉS AZ INFORMÁCIÓK VÉDELME

19. cikk

A nyilvántartások megőrzése

(1) A nemzeti tanúsítási rendszerek követelményeket tartalmaznak a tanúsító szervek számára az általuk végzett megfelelőségértékelési tevékenységekkel kapcsolatban előállított valamennyi releváns információ nyilvántartási rendszerére vonatkozóan, beleértve az adattárca-megoldások a megoldások szolgáltatására használt elektronikus azonosítási rendszerek szolgáltatói által kiállított, illetve kapott adatokat. Az ezeket az információkat tartalmazó nyilvántartásokat biztonságos módon kell tárolni. A nyilvántartások tárolása elektronikus úton is történhet; az információknak az uniós vagy a nemzeti jog által előírt ideig, valamint az adott megfelelőségi tanúsítvány törlését vagy lejártát követően legalább öt évig hozzáférhetőnek kell maradniuk.

(2) A nemzeti tanúsítási rendszerek követelményeket állapítanak meg a megfelelőségi tanúsítvány jogosultjai számára arra vonatkozóan, hogy e rendelet alkalmazásában és az adott megfelelőségi tanúsítvány törlését vagy lejártát követően legalább öt évig biztonságosan tárolják a következőket:

a) a tanúsító szerv vagy annak bármely alvállalkozója számára a tanúsítási folyamat során szolgáltatott információk;

b) az adattárca-megoldás tanúsításának tárgyát képező hardverkomponensek egy-egy példánya.

(3) A nemzeti tanúsítási rendszerek előírják a megfelelőségi tanúsítvány jogosultja számára, hogy kérésre bocsássa az (1) bekezdésben említett információkat a tanúsító szerv vagy a 910/2014/EU rendelet 46a. cikkének (1) bekezdésében említett felügyeleti szerv rendelkezésére.

20. cikk

Az információk védelme

A nemzeti tanúsítási rendszerek keretében minden olyan személy vagy szervezet, aki, illetve amely a nemzeti tanúsítási rendszer keretében végzett tevékenységek végrehajtása során hozzáféréssel rendelkezik az információkhoz, köteles biztosítani az üzleti titkok és egyéb bizalmas adatok biztonságát és védelmét, valamint a szellemitulajdon-jogok megőrzését, és köteles megtenni a szükséges és megfelelő technikai és szervezési intézkedéseket a titoktartás biztosítása érdekében.

IX. FEJEZET

ZÁRÓ RENDELKEZÉSEK

21. cikk

Áttérés az európai kiberbiztonsági tanúsítási rendszerre

Az adattárca-megoldásokra és a megoldások szolgáltatására használt elektronikus azonosítási rendszerekre vonatkozó első európai kiberbiztonsági tanúsítási rendszer elfogadásakor ezt a rendeletet felül kell vizsgálni a tekintetben, hogy egy ilyen európai kiberbiztonsági tanúsítási rendszer milyen mértékben járul hozzá az adattárca-megoldások és a megoldások szolgáltatására használt elektronikus azonosítási rendszerek általános tanúsításához.

22. 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, 2024. november 28-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

I. MELLÉKLET

KOCKÁZAT-NYILVÁNTARTÁS AZ EURÓPAI DIGITÁLIS SZEMÉLYIADAT-TÁRCÁKHOZ

Bevezetés

A kockázat-nyilvántartás az adattárcákra vonatkozó azon főbb biztonsági és adatvédelmi kockázatokat és veszélyforrásokat ismerteti, amelyeket az adattárcák minden architektúrájában és implementációjában megfelelően kezelni kell. Az adattárcák felhasználók és igénybe vevő felek általi használatához kapcsolódó **magas szintű kockázatok** (I. szakasz) az adattárcákban lévő eszközöket megcélzó közvetlen veszélyforrásokhoz társulnak. Emellett azonosítottak néhány olyan, az adattárcákat érintő **rendszerszintű kockázatot** (II. szakasz), amelyek jellemzően a teljes adattárcarendszerre vonatkozó veszélyforrások kombinációjából erednének.

Kockázat típusa	Kockázatazonosító	Kapcsolódó kockázatok megnevezése
Az adattárcákat érintő magas szintű kockázatok	R1	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása
	R2	Hamis elektronikus személyazonosság létrehozása vagy felhasználása
	R3	Hamis attribútum létrehozása vagy felhasználása
	R4	Személyazonosság-lopás
	R5	Adatlopás
	R6	Adatok közzététele
	R7	Adatmanipulálás
	R8	Adatvesztés
	R9	Nem engedélyezett tranzakció
	R10	Tranzakciómanipulálás
	R11	Letagadhatóság
	R12	Tranzakcióadatok közzététele
	R13	Szolgáltatás zavara
	R14	Megfigyelés
A rendszerrel összefüggő kockázatok	SR1	Tömeges megfigyelés
	SR2	Jó hírnév megsértése
	SR3	Jogszabályoknak való meg nem felelés

A nyilvántartás az adattárca-megoldás megvalósítását célzó **technikai veszélyforrásokat** is azonosít (III. szakasz). Ezek a veszélyforrások a magas szintű kockázatokkal függnek össze olyan értelemben, hogy mindegyikük számos magas szintű kockázat előidézésére használható.

Veszélyforrás típusa	Veszélyforrás-azonosító	Kapcsolódó veszélyforrások megnevezése	Veszélyforrások alkategóriái
Technikai veszélyforrás	TT1	Fizikai támadás	1.1. *Lopás*
			1.2. *Információk kiszivárgása*
			1.3. *Illetéktelen módosítás*
	TT2	Hiba és hibás konfiguráció	2.1. *Informatikai rendszer kezelése során elkövetett hiba*
			2.2. *Alkalmazásszintű hiba vagy felhasználási hiba*
			2.3. *Fejlesztési hiba és rendszerhiba*

Veszélyforrás típusa	Veszélyforrás-azonosító	Kapcsolódó veszélyforrások megnevezése	Veszélyforrások alkategóriái
	TT3	Megbízhatatlan erőforrás használata	3.1. *Adattárca-összetevők hibás használata vagy konfigurációja*
	TT4	Meghibásodás és üzemszünet	4.1. *Berendezés, eszköz vagy rendszer meghibásodása vagy működési zavara*
			4.2. *Erőforrások kiesése*
			4.3. *Támogatási szolgáltatások kiesése*
	TT5	Rosszindulatú tevékenység	5.1. *Információk kifürkészése*
			5.2. *Adathalászat és hamisítás*
			5.3. *Üzenetek visszajátszása*
			5.4. *Próbálgatásos támadás*
			5.5. *Szoftverek sebezhetősége*
			5.6. *Ellátási láncok ellen elkövetett támadás*
			5.7. *Kártékony szoftver*
			5.8. *Véletlenszerű számok feltörése*

Végezetül a nyilvántartás felsorolja **az adattárcákat fenyegető közvetlen veszélyforrásokat**, mindegyiknél megadva (a teljesség igénye nélkül) a kapcsolódó kockázatokat (IV. szakasz).

I. SZAKASZ

Az adattárcákat érintő magas szintű kockázatok

R1. Meglévő elektronikus személyazonosság létrehozása vagy felhasználása

A meglévő elektronikus személyazonosság létrehozása vagy felhasználása egy elektronikus személyazonosságnak a valóságban létező, másik felhasználóhoz hozzárendelt adattárcában történő létrehozása. Ez a kockázat lényegében a személyazonosság-lopás (R4) és a nem engedélyezett tranzakció (R9) kockázatához vezet.

R2. Hamis elektronikus személyazonosság létrehozása vagy felhasználása

A hamis elektronikus személyazonosság létrehozása vagy felhasználása egy elektronikus személyazonosságnak a valóságban nem létező adattárcában történő létrehozása.

R3. Hamis attribútum létrehozása vagy felhasználása

A hamis attribútum létrehozása vagy felhasználása olyan attribútum létrehozása vagy felhasználása, amelynek az állítólagos szolgáltató általi kibocsátását nem lehet érvényesíteni, így nem megbízható.

R4. Személyazonosság-lopás

A személyazonosság-lopás az adattárcaegység engedély nélküli megszerzése vagy a hitelesítési tényezőknek a személyazonossággal való visszaélést lehetővé tevő elvesztése.

R5. Adatlopás

Az adatlopás az adatok engedély nélküli kinyerése. Az adatlopás olyan veszélyforrásokhoz is kötődik, mint például az adatkifürkészés (az átvitel alatt lévő adatok illetéktelen rögzítése) és az adatok dekódolása (a titkosított adatok nem engedélyezett visszafejtése), amelyek egyes esetekben valószínűleg adatok közzétételéhez (R6) vezetnek.

R6. Adatok közzététele

Az adatok közzététele a személyes adatok jogosulatlan hozzáférhetővé tétele, beleértve a személyes adatok különleges kategóriáit is. A magánélet tiszteletben tartásához való jog megsértésének kockázata nagyon hasonló ehhez, ha a magánélet védelme, nem pedig a biztonság szempontjából szemléljük.

R7. Adatmanipulálás

Az adatmanipulálás az adatok jogosulatlan megváltoztatása.

R8. Adatvesztés

Adatvesztés az a helyzet, amikor az adattárcában tárolt adatok visszaélés vagy rosszindulatú tevékenység miatt elvesznek. Ez a kockázat gyakran az adatmanipulálásnak (R7) vagy a szolgáltatás zavarának (R13) olyan másodlagos kockázata, amelynek esetében az összes adat vagy egy részük nem állítható helyre.

R9. Nem engedélyezett tranzakció

A nem engedélyezett tranzakció olyan működtetési tevékenység, amelyet az adattárca-felhasználó engedélye vagy tudomása nélkül végeznek. A nem engedélyezett tranzakció sok esetben személyazonosság-lopáshoz (R4) vagy adatok közzétételéhez (R6) vezethet. Olyan nem engedélyezett tranzakciókhoz is kapcsolódik, mint például a kriptográfiai kulccsal való visszaélés.

R10. Tranzakciómanipulálás

A tranzakciómanipulálás az adattárcában szereplő tranzakciók engedély nélküli megváltoztatása. A tranzakciómanipulálás az integritás elleni támadás, az adatintegritás sérüléséhez hasonló kockázat.

R11. Letagadhatóság

A letagadhatóság olyan helyzet, amelyben az érdekelt fél tagadhatja, hogy végrehajtott egy műveletet, vagy részt vett egy tranzakcióban, és más érdekelt felek nem rendelkeznek kellő bizonyítékkal ahhoz, hogy ezt cáfolják.

R12. Tranzakcióadatok közzététele

A tranzakcióadatok közzététele az érdekelt felek közötti tranzakciókra vonatkozó információk közzététele.

R13. Szolgáltatás zavara

A szolgáltatás zavara az adattárca szokásos működésének megszakadása vagy romlása. A szolgáltatás zavarának sajátos válfaja a felhasználók kizárása, mely esetben a felhasználó képtelen hozzáférni fiókjához vagy adattárcájához.

R14. Megfigyelés

A megfigyelés vagy figyelés az adattárca-felhasználó tevékenységének, kommunikációjának vagy adatainak engedély nélküli nyomon követése vagy figyelemmel kísérése. Gyakran kötődik a dedukcióhoz, amely a különleges vagy személyes adatoknak a látszólag ártalmatlan adatokból való kikövetkeztetése.

II. SZAKASZ

A rendszerrel összefüggő kockázatok

Ezek a kockázatok nem szerepelnek a veszélyforrások listáján, mivel általában több veszélyforrás következményei, amelyek a teljes rendszert fenyegető módon ismétlődnek.

SR1. Tömeges megfigyelés

A tömeges megfigyelés sok felhasználó tevékenységének nyomon követése vagy figyelemmel kísérése az adattárcáik kommunikációja vagy adatai alapján. A tömeges megfigyelés gyakran kötődik megfigyeléshez (R14) és globális szintű dedukcióhoz, amelynek során számos felhasználóra vonatkozó információt kombinálnak a felhasználókra vonatkozó különleges vagy személyes adatok kikövetkeztetése vagy további támadások megtervezésére felhasználható statisztikai tendenciák azonosításához.

SR2. Jó hírnév megsértése

A jó hírnév megsértése a szervezet vagy kormányzati szerv jó hírnevének sérelme. A jó hírnév megsértése egyéb kockázatokból is ered, amikor a média beszámol egy adatvédelmi incidensről vagy biztonsági eseményről, és kedvezőtlen fényben tünteti fel a szervezetet. A jó hírnév megsértése további kockázatokhoz vezethet, például a felhasználó alapos kétségeiből eredő bizalomvesztéshez és az ökoszisztéma elvesztéséhez, amikor a teljes ökoszisztéma összeomlik.

SR3. Jogszabályoknak való meg nem felelés

A jogszabályoknak való meg nem felelés olyan helyzet, amikor a vonatkozó törvények, rendeletek vagy szabványok nem tarthatók be. Mivel a megoldás biztonságossága és adatvédelme az adattárcával összefüggésben jogi követelmény, ez esetben minden veszélyforrás valószínűleg valamilyen jogszabálynak való meg nem feleléshez vezet.

III. SZAKASZ

Technikai veszélyforrás

A technikai veszélyforrások nem minden esetben kötődnek az adattárcát érintő konkrét kockázatokhoz, mivel sokuk olyan eszköz, amely számos különböző kockázatnak megfelelő támadás végrehajtására használható.

TT1. Fizikai támadás

1.1. *Lopás*

A lopás olyan eszközök eltulajdonítása, amelyek módosíthatják az adattárca megfelelő működését (amennyiben az eszközt ellopják, és az adattárcaegység nem kap kellő védelmet). Ez számos kockázathoz hozzájárulhat, ideértve a személyazonosság-lopást (R4), az adatlopást (R5) és a nem engedélyezett tranzakciókat (R9).

1.2. *Információk kiszivárgása*

Az információk kiszivárgása az adattárcához való fizikai hozzáférést követő jogosulatlan hozzáférés, információk hozzáférhetővé tétele vagy megosztása. Különösen az adatok közzétételéhez (R6) és az adatlopáshoz (R5) járulhat hozzá.

1.3. *Illetéktelen módosítás*

Az illetéktelen módosítás az adattárcaegység egy vagy több összetevője vagy azon összetevők integritásának megsértése, amelyekre az adattárcaegység támaszkodik, pl. a felhasználói eszköz vagy annak operációs rendszere. Különösen az adatmanipuláláshoz (R7), az adatvesztéshez (R8) és a tranzakciómanipuláláshoz (R10) járulhat hozzá. Ha az illetéktelen módosításnak szoftverkomponens a célpontja, az számos kockázathoz járulhat hozzá.

TT2. Hiba és hibás konfiguráció

2.1. *Informatikai rendszer kezelése során elkövetett hiba*

Az informatikai rendszer kezelése során elkövetett hiba az információk olyan kiszivárgása, megosztása vagy az azokban bekövetkezett olyan kár, amelynek oka az informatikai eszközöknek a felhasználók általi helytelen használata (az alkalmazásjellemzők ismeretének hiánya), illetve az informatikai eszközök nem megfelelő konfigurációja vagy kezelése.

2.2. *Alkalmazásszintű hiba vagy felhasználási hiba*

Az alkalmazásszintű hiba vagy felhasználási hiba az alkalmazás olyan működési zavara, amely magának az alkalmazásnak a hibájából vagy az egyik felhasználó (adattárca-felhasználó vagy igénybe vevő fél) hibájából ered.

2.3. *Fejlesztési hiba és rendszerhiba*

A fejlesztési hiba és rendszerhiba a nem megfelelően fejlesztett vagy konfigurált informatikai eszközök vagy üzleti folyamatok (az informatikai termékek nem megfelelő specifikációi, elégtelen használhatóság, nem biztonságos felhasználói felület, nem megfelelő házirend- és eljárási folyamatok, tervezési hibák) által okozott működési zavar vagy sebezhetőség.

TT3. Megbízhatatlan erőforrás használata

A megbízhatatlan erőforrás használata olyan nem szándékos kárhoz vezető tevékenység, amely rosszul meghatározott bizalmi kapcsolatokból ered, mint amilyen például a harmadik fél szolgáltatóba elegendő bizonyosság szerzése nélkül vetett bizalom.

3.1. *Adattárca-összetevők hibás használata vagy konfigurációja*

Az adattárca-összetevők hibás használata vagy konfigurációja az adattárca összetevőiben nem szándékosan okozott kár, amely az adattárca-felhasználók vagy nem megfelelően képzett fejlesztők általi hibás használatból vagy konfigurálásból, illetve a fenyegetettségi helyzet változásaihoz való alkalmazkodás hiányából, jellemzően harmadik felek sérülékeny összetevőinek vagy futásidejű platformjainak a használatából ered.

TT4. Meghibásodás és üzemszünet

4.1. *Berendezés, eszköz vagy rendszer meghibásodása vagy működési zavara*

A berendezés meghibásodása vagy működési zavara a berendezések – többek között a szolgáltató infrastruktúrája és a felhasználói eszközök – meghibásodása vagy hibás működése miatt az informatikai eszközökben nem szándékosan okozott kár.

4.2. *Erőforrások kiesése*

Az erőforrások kiesése az erőforrások – például karbantartáshoz szükséges alkatrészek – rendelkezésre állásának hiánya miatti üzemszünet vagy működési zavar.

4.3. *Támogatási szolgáltatások kiesése*

A támogatási szolgáltatások kiesése a rendszer helyes működéséhez szükséges támogatási szolgáltatásoknak – többek között a szolgáltatói infrastruktúra és a felhasználói eszköz hálózati kapcsolatának – a rendelkezésre nem állása miatti üzemszünet vagy működési zavar.

TT5. Rosszindulatú tevékenység

5.1. *Információk kifürkészése*

Az információk kifürkészése az átvitel során nem megfelelően védett információk megszerzése, beleértve a közbeékelődéses támadást is.

5.2. *Adathalászat és hamisítás*

Az adathalászat a felhasználó által nyújtott információk megtévesztő interakciót követő megszerzése, amely gyakran kötődik a legitim kommunikációs eszközök és webhelyek meghamisításához. Ezeknek a veszélyforrásoknak a felhasználó a célpontja, és jellemzően a személyazonosság-lopás (R4) és a nem engedélyezett tranzakciók (R9) kockázatához járulnak hozzá, gyakran adatlopás (R5) vagy adatok közzététele (R6) révén.

5.3. *Üzenetek visszajátszása*

Az üzenetek visszajátszása a korábban elfogott üzenetek újrafelhasználása nem engedélyezett tranzakciók végrehajtása céljából, ami gyakran protokollszinten történik. Ez a technikai veszélyforrás főként a nem engedélyezett tranzakciók kockázatához járul hozzá, ami a tranzakciótól függően más kockázatokhoz vezethet.

5.4. *Próbálgatásos támadás*

A próbálgatásos támadás a biztonság és gyakran a titoktartás megsértése, amelynek során nagyszámú interakciót folytatnak mindaddig, amíg a válasz értékes információval nem szolgál.

5.5. *Szoftverek sebezhetősége*

A szoftverek sebezhetőségével kapcsolatos veszélyforrás a biztonság megsértése az adattárca összetevőiben vagy az adattárca megvalósításához használt szoftver- és hardverkomponensekben található szoftveres sérülékenység kiaknázása révén, beleértve a közzétett és a közzé nem tett (nulladik napi) biztonsági réseket is.

5.6. *Ellátási láncok ellen elkövetett támadás*

Az ellátási láncok ellen elkövetett támadás a biztonság megsértése az adattárca-szolgáltatónak vagy a szolgáltató felhasználóinak a beszállítója ellen elkövetett olyan támadások révén, amelyek célja, hogy lehetővé tegyék az adattárca elleni további közvetlen támadásokat.

5.7. *Kártékony szoftver*

A kártékony szoftver a biztonság olyan rosszindulatú alkalmazások révén történő megsértése, amelyek nem kívánt és illegitim műveleteket hajtanak végre az adattárca ellen.

5.8. *Véletlenszerű számok feltörése*

A véletlenszerű számok feltörése a próbálgatásos támadásoknak a véletlenszerűen generált számok részleges vagy teljes előrejelzése révén történő lehetővé tétele.

IV. SZAKASZ

Az adattárcákat fenyegető veszélyforrások

Az utolsó szakasz az adattárcákra jellemző fenyegetettségi forgatókönyveket mutat be, az azokhoz köthető, fentiekben felsorolt főbb magas szintű kockázatokkal párosítva. A lista tartalmazza azokat a veszélyforrásokat, amelyekkel szemben fel kell lépni, ám nem képezi a veszélyforrások teljeskörű listáját, amely nagymértékben függ a kiválasztott adattárca-megoldás architektúrájától és a fenyegetettségi környezet alakulásától. Emellett a kockázatértékelést és a javasolt intézkedéseket illetően az adattárca-szolgáltató csak a tanúsítás tárgyát képező összetevőkért vonható felelősségre (*).

Azonosító *Azonosító*	Veszélyforrás leírása *Az azonosított veszélyforrás ismertetése (*)*	Kockázat megnevezése *Kapcsolódó kockázatok*
TR1	A támadó alapos ok nélkül visszavonhat álneveket.	Hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)
TR2	A támadó hamis, nem létező elektronikus személyazonosságot állíthat ki.	Hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)
TR3	A támadó engedély nélküli személyazonosító adatokat kezdhet kiállítani.	Hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)
TR4	A támadó ráveheti a rendszergazdát, hogy rossz személyazonosítóadat-szolgáltatót vigyen fel a megbízható személyazonosítóadat-szolgáltatók listájára.	Hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)
TR5	A támadó megkerülheti a távoli személyazonosság-igazolási szolgáltatást.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)
TR6	A támadó megkerülheti a fizikai személyazonosság-igazolási szolgáltatást.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)
TR7	A támadó megkerülheti a távoli (minősített) tanúsítvány használatával kapcsolatos személyazonosság-igazolási szolgáltatásokat.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)
TR8	A támadó hozzáférhet a személyhez nem kötött adattárcákhoz.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)
TR9	A támadó helytelen személyazonosító adatok létrehozása céljából kijátszhatja a technikai és eljárásbeli ellenőrzéseket.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)
TR10	A támadó új adattárcát aktiválhat egy érvénytelen adattárca-biztonsági kriptográfiai eszközön.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)
TR11	A támadó megkerülheti a meglévő elektronikus személyazonosítási eszközök használatával kapcsolatos személyazonosság-igazolási szolgáltatást.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ személyazonosság-lopás (R4)/nem engedélyezett művelet (R9)
TR12	A támadó megkerülheti annak a személyazonosítóadat-szolgáltató által végzett ellenőrzését, hogy az adattárca a felhasználó ellenőrzése alatt áll-e, és személyazonosító adatot állíttathat ki a támadó ellenőrzése alatt álló, feltört adattárcába.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ személyazonosság-lopás (R4)/nem engedélyezett művelet (R9)

Azonosító *Azonosító*	Veszélyforrás leírása *Az azonosított veszélyforrás ismertetése (*)*	Kockázat megnevezése *Kapcsolódó kockázatok*
TR13	A támadó érvényes személyazonosító adatot szerezhet egy érvénytelen adattárcaegységbe.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ személyazonosság-lopás (R4)/nem engedélyezett művelet (R9)
TR14	A személyazonosítóadat-szolgáltató hamis személyazonosságot állíthat ki, ahol a személyazonosság létező személyhez kapcsolódik.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ személyazonosság-lopás (R4)/nem engedélyezett művelet (R9)
TR15	A támadó helytelen adattárcával kapcsolhat össze egy személyazonosító adatot, mivel a személyazonosítóadat-szolgáltató nem tudja a megfelelő adattárcához kötni a személyazonosító adatot.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ személyazonosság-lopás (R4)/nem engedélyezett művelet (R9)
TR16	A támadó ráveheti a felhasználót, hogy hagyja jóvá a támadó ellenőrzése alatt álló új adattárcaegység/példány aktiválását – a tanúsítványok utólagos ellenőrzésével együtt.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ hamis elektronikus személyazonosság létrehozása vagy felhasználása (R2)/ személyazonosság-lopás (R4)/nem engedélyezett művelet (R9)
TR17	A támadó kiállíthat másik állambeli személyazonosító adatokat, hogy hozzáférjen a célba vett polgárok adataihoz/ digitális eszközeihez.	Meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)/ személyazonosság-lopás (R4)/nem engedélyezett művelet (R9)
TR18	A támadó hamis (minősített) elektronikus attribútumtanúsítványok létrehozása céljából kijátszhatja a technikai és eljárásbeli ellenőrzéseket.	Hamis attribútum létrehozása vagy felhasználása (R3)
TR19	A támadó a részére nem érvényesen kiállított (minősített) elektronikus attribútumtanúsítványokat jeleníthet meg.	Hamis attribútum létrehozása vagy felhasználása (R3)
TR20	A támadó megtámadhatja az adattárcának a személyazonosító adat és egy olyan (minősített) elektronikus attribútumtanúsítvány közötti kriptográfiai összekapcsoló mechanizmusát, amely nem állítható ki neki.	Hamis attribútum létrehozása vagy felhasználása (R3)
TR21	A támadó olyan (minősített) elektronikus attribútumtanúsítványt használhat az adattárcában, amelynek fizikai megfelelője lejárt vagy érvénytelen.	Hamis attribútum létrehozása vagy felhasználása (R3)
TR22	A támadó megkerülheti annak a (minősített) elektronikus attribútumtanúsítvány szolgáltatója által végzett ellenőrzését, hogy az adattárca a felhasználó ellenőrzése alatt áll-e, és (minősített) elektronikus attribútumtanúsítványt állíttathat ki a támadó ellenőrzése alatt álló, feltört adattárcába.	Hamis attribútum létrehozása vagy felhasználása (R3)
TR23	A támadó elektronikus attribútumtanúsítványokat hamisíthat.	Hamis attribútum létrehozása vagy felhasználása (R3)
TR24	A támadó hamisított elektronikus attribútumtanúsítványokat juttathat be az adattárcába.	Hamis attribútum létrehozása vagy felhasználása (R3)
TR25	Az adattárca a felhasználó jóváhagyása nélkül jeleníthet meg attribútumokat az igénybe vevő félnek.	Adatok közzététele (R6)
TR26	Személyazonosító adatok, (minősített) elektronikus attribútumtanúsítványok vagy álnevek jeleníthetők meg egy téves igénybe vevő félnek.	Adatok közzététele (R6)
TR27	A támadó az elektronikus attribútumtanúsítvány rosszindulatú megújítását kezdeményezheti.	Adatok közzététele (R6)
TR28	A támadó (adathalászattal vagy más módon) ráveheti a felhasználót, hogy tévesen jóváhagyjon egy elektronikus attribútumtanúsítvány iránti kérelmet.	Adatok közzététele (R6)

Azonosító *Azonosító*	Veszélyforrás leírása *Az azonosított veszélyforrás ismertetése (*)*	Kockázat megnevezése *Kapcsolódó kockázatok*
TR29	A támadó attribútumokat szivárogtathat ki az adattárcából, és azonosíthatja az adattárca felhasználóját, amennyiben nem szükséges/engedélyezett az azonosítás.	Adatok közzététele (R6)
TR30	A támadó adatok kinyerése céljából kijátszhatja a technikai és eljárásbeli ellenőrzéseket.	Adatok közzététele (R6)
TR31	Kérelmek szivárogtathatók ki a támadóhoz.	Adatok közzététele (R6)
TR32	A támadó ismereteket szerezhet az attribútumokra vonatkozó beágyazott közzétételi szabályzatról, és az adattárcaegységek jelenlegi kérelmében szereplő attribútumokat jeleníthet meg.	Adatok közzététele (R6)
TR33	A támadó kinyerhet naplókat vagy azok részeit az eszközről.	Adatok közzététele (R6)
TR34	A támadó megtudhatja, hogy az adattárcát az általa használttal azonos eszközre vagy másikra telepítették-e, és hozzájuthat az azon tárolt információkhoz.	Adatok közzététele (R6)
TR35	A támadó megszerezheti a felhasználó adattárca-biztonsági kriptográfiai alkalmazásban történő hitelesség-ellenőrzéséhez használt tudásfaktort (azaz ismeretet).	Adatok közzététele (R6)
TR36	Adott személy olyan elektronikus attribútumtanúsítványa, amelyet egy igénybe vevő féllel folytatott több tranzakcióban vagy különböző igénybe vevő feleknek jelenítenek meg, akaratlanul lehetővé teszi, hogy több tranzakciót az érintett személyhez kössenek.	Adatok közzététele (R6)
TR37	A visszavont tanúsítványok/igénybe vevő felek nyilvános listája információkat tartalmazhat arról, hogy a felhasználó hogyan használja a tanúsítványát (pl. tartózkodási hely, IP-cím stb.).	Adatok közzététele (R6)
TR38	Ha az igénybe vevő felek nem tudják bizonyítani, hogy a felhasználó hozzájárult a megosztott attribútumokhoz, az kihathat a naplók integritására.	Adatok közzététele (R6)
TR39	A támadó egyedi/nyomon követhető azonosítók használatával jogellenesen nyomon követheti az adattárca-felhasználókat.	Adatok közzététele (R6)/megfigyelés (R14)
TR40	A több, különböző engedélyezett kérelmezési/feldolgozási körű egységből/szervezetből álló igénybe vevő fél olyan adatokat is kérelmezhet és feldolgozhat, amelyekre nincs jogszerű indoka.	Adatok közzététele (R6)/nem engedélyezett tranzakció (R9)
TR41	A támadó úgy szabotálhatja a személyi azonosítók adattárca általi integritás- és hitelesség-ellenőrzéseit, hogy mindig sikeres eredményt adjanak.	Adatmanipulálás (R7)
TR42	A támadó megkerülheti vagy szabotálhatja a kérelmezett attribútumok integritásának és hitelességének adattárca általi ellenőrzéseit, hogy mindig sikeres eredményt adjanak.	Adatmanipulálás (R7)
TR43	A támadó megkerülheti vagy szabotálhatja az azonos felhasználóhoz tartozó összes kérelmezett attribútum adattárca általi ellenőrzéseinek elvégzését, hogy mindig sikeres eredményt adjanak.	Adatmanipulálás (R7)
TR44	A támadó megkerülheti vagy szabotálhatja a személyazonosító adatok érvényességének és megbízható személyazonosítóadat-szolgáltató általi kiállításának adattárca általi ellenőrzéseit, hogy mindig sikeres eredményt adjanak.	Adatmanipulálás (R7)

Azonosító *Azonosító*	Veszélyforrás leírása *Az azonosított veszélyforrás ismertetése (*)*	Kockázat megnevezése *Kapcsolódó kockázatok*
TR45	A támadó megkerülheti vagy szabotálhatja a minősített elektronikus attribútumtanúsítvány érvényességének és a minősített elektronikus attribútumtanúsítvány kibocsátására nyilvántartásba vett, minősített bizalmi szolgáltató általi kiállításának adattárca általi ellenőrzéseit, hogy mindig sikeres eredményt adjanak.	Adatmanipulálás (R7)
TR46	A támadó megkerülheti vagy szabotálhatja a személyazonosító adatok személyazonosítóadat-szolgáltató általi visszavonásának adattárca általi ellenőrzéseit, hogy mindig sikeres eredményt adjanak.	Adatmanipulálás (R7)
TR47	A támadó megkerülheti vagy szabotálhatja a (minősített) elektronikus attribútumtanúsítványnak a (minősített) elektronikus attribútumtanúsítvány szolgáltatója általi visszavonása adattárca általi ellenőrzéseit, hogy mindig sikeres eredményt adjanak.	Adatmanipulálás (R7)
TR48	A támadó módosíthatja az elviekben kizárólag a felhasználó ellenőrzése alatt álló biztonsági mentési és helyreállítási adatok tartalmát.	Adatmanipulálás (R7)/adatvesztés (R8)
TR49	A támadó módosíthatja egy adott adattárcapéldány tevékenységnaplókból származó tranzakcióelőzményeit.	Adatmanipulálás (R7)/adatvesztés (R8)
TR50	A támadó lehallgathatja az adattárca és az igénybe vevő felek közötti kapcsolatot.	Adatlopás (R5)/adatok közzététele (R6)
TR51	A támadó ráveheti a felhasználót arra, hogy ossza meg a személyes adatait (pl. személyazonosító adatot, elektronikus attribútumtanúsítványt, álnevet, elektronikus aláírást, naplót vagy más adatot) a támadóval vagy olyan harmadik féllel, akivel nincs szándékában.	Adatlopás (R5)/adatok közzététele (R6)
TR52	A támadó elolvashatja egy adott adattárcapéldány tevékenységnaplókból származó tranzakcióelőzményeit.	Adatlopás (R5)/adatok közzététele (R6)
TR53	A támadó kriptográfiai kulcsok anyagát exportálhatja vagy vonhatja ki az adattárca-biztonsági kriptográfiai eszközből.	Adatlopás (R5)/adatok közzététele (R6)/ nem engedélyezett tranzakció (R9)
TR54	A támadó elolvashatja az elviekben kizárólag a felhasználó ellenőrzése alatt álló biztonsági mentési és helyreállítási adatok tartalmát.	Adatlopás (R5)/adatok közzététele (R6)
TR55	A támadó megkerülheti a felhasználói hitelesség ellenőrzési módszerét az adattárcaegység által generált álnév használatához.	Személyazonosság-lopás (R4)
TR56	A támadó olyan alkalmazást ajánlhat a felhasználóknak, amely egy konkrét, legitim adattárcát utánoz.	Személyazonosság-lopás (R4)
TR57	A támadó adattárcaadatokat, többek között személyazonosító adatokat, (minősített) elektronikus attribútumtanúsítványokat vagy naplókat exportálhat.	Személyazonosság-lopás (R4)
TR58	A támadó kriptográfiai összeköttetési anyagot exportálhat.	Személyazonosság-lopás (R4)
TR59	A támadó az adattárca kriptográfiai kulcsain keresztül személyazonosságokat sajátíthat ki.	Személyazonosság-lopás (R4)
TR60	A támadó a személyes eszközén használható másolatot készíthet más felhasználó személyes adattárcaegységéről.	Személyazonosság-lopás (R4)/meglévő elektronikus személyazonosság létrehozása vagy felhasználása (R1)

Azonosító *Azonosító*	Veszélyforrás leírása *Az azonosított veszélyforrás ismertetése (*)*	Kockázat megnevezése *Kapcsolódó kockázatok*
TR61	Egy másik állam hatósága arra kérheti a felhasználót, hogy mutassa be, illetve ossza meg az adattárca összes adatát a fizikai térben, például az adott állam határának átlépésekor.	Személyazonosság-lopás (R4)/ megfigyelés (R14)
TR62	A felhasználók a felhasználói eszköz meghibásodása után nem tudják átvinni a tranzakciós naplóikat az új adattárcára, így azon nem lehet nyomon követni a korábbi tranzakciókat.	Letagadhatóság (R11)
TR63	A felhasználók a felhasználói eszköz meghibásodása után nem tudják helyreállítani a tranzakciós naplóikat, így azokat nem lehet nyomon követni az új adattárcán.	Letagadhatóság (R11)
TR64	Az igénybe vevő felek nehezen tudják bizonyítani a távoli elektronikus aláíráshoz való hozzájárulást.	Letagadhatóság (R11)
TR65	A támadó az igénybe vevő felekhez való csatlakozás során kérelmekkel áraszthatja el a kapcsolatot vagy kapcsolatokat.	Szolgáltatás zavara (R13)
TR66	A támadó az igénybe vevő felekhez való csatlakozásokkal áraszthatja el a státuszbiztosítási szolgáltatást.	Szolgáltatás zavara (R13)
TR67	A támadó az attribútummegjelenítést kétségbevonhatóként/ elutasítottként tüntetheti fel, annak ellenére, hogy az attribútum a megjelenítése alapján érvényes.	Szolgáltatás zavara (R13)
TR68	A támadó alapos ok nélkül visszavonhat személyazonosító adatokat.	Szolgáltatás zavara (R13)
TR69	A támadó a felhasználó hozzájárulása nélkül visszavonhat személyazonosító adatokat.	Szolgáltatás zavara (R13)
TR70	A támadó alapos ok nélkül visszavonhat (minősített) elektronikus attribútumtanúsítványokat.	Szolgáltatás zavara (R13)
TR71	A támadó a felhasználó hozzájárulása nélkül visszavonhat (minősített) elektronikus attribútumtanúsítványokat.	Szolgáltatás zavara (R13)
TR72	A támadó több azonosítási kérelmet is kezdeményezhet anélkül, hogy a rendszer felismerné, hogy azok szándékos árva kérelmek.	Szolgáltatás zavara (R13)
TR73	A támadó több kérelmet is küldhet nyomonkövetési tranzakció nélkül.	Szolgáltatás zavara (R13)
TR74	A támadó lehetővé teheti, hogy az igénybe vevő fél megfeleltetett azonosítás (válasz) és teljeskörű ellenőrzés nélkül kérjen azonosítást.	Szolgáltatás zavara (R13)
TR75	A támadó az időkorlát lejárta után vagy hasonló helyzetekben válaszolhat egy kérelemre, ami a szolgáltatás zavarához vezet.	Szolgáltatás zavara (R13)
TR76	Az igénybe vevő fél több érvénytelen kérelmet is küldhet.	Szolgáltatás zavara (R13)
TR77	A támadó több érvénytelen kérelmet is küldhet az adattárca-szolgáltatónak.	Szolgáltatás zavara (R13)
TR78	A támadó meggátolhatja, hogy a tagállamok nem megbízható személyazonosítóadat-szolgáltatókat vonjanak vissza a megbízható személyazonosítóadat-szolgáltatók listájáról.	Szolgáltatás zavara (R13)
TR79	A támadó megakadályozhatja az adattárca felfüggesztését vagy visszavonását.	Szolgáltatás zavara (R13)

Azonosító *Azonosító*	Veszélyforrás leírása *Az azonosított veszélyforrás ismertetése (*)*	Kockázat megnevezése *Kapcsolódó kockázatok*
TR80	A támadó letilthatja az igénybe vevő felek, felhasználók és/vagy személyazonosítóadat-szolgáltatók tranzakcióit.	Szolgáltatás zavara (R13)
TR81	A támadó letilthatja vagy hozzáférhetetlenné teheti az adattárca-biztonsági kriptográfiai eszközöket.	Szolgáltatás zavara (R13)
TR82	A támadó megakadályozhatja, hogy a személyazonosítóadat-szolgáltató személyazonosító adatokat vonjon vissza vagy függesszen fel.	Szolgáltatás zavara (R13)/nem engedélyezett tranzakció (R9)
TR83	Az igénybe vevő fél a vele megosztott adatokon túlmenően is kikövetkeztetheti a felhasználó személyazonosító adatait.	Megfigyelés (R14)
TR84	Az összejátszó igénybe vevő felek vagy személyazonosítóadat-szolgáltatók egy csoportja a számára ismert adatokon túlmenően is kikövetkeztetheti a felhasználó személyazonosító adatait.	Megfigyelés (R14)
TR85	A támadó a felhasználó személyazonosító adatainak felhasználásával nyomon követheti a felhasználót, amennyiben nem szükséges a felhasználó azonosítása.	Megfigyelés (R14)
TR86	A támadó a (minősített) elektronikus attribútumtanúsítványok kombinációjával „hamisított” megjelenítést végezhet.	Tranzakciómanipulálás (R10)
TR87	A támadó a felhasználó kifejezett hozzájárulása vagy kizárólagos ellenőrzése nélkül távolról aktiválhatja/kisajátíthatja az adattárcát (pl. hitelesítési vagy tanúsítványkérelmet beágyazó banki alkalmazást) olyan helyzetben, amikor a felhasználó nincs ennek tudatában (pl. alszik), vagy nem látja az igénybe vevő felet.	Tranzakciómanipulálás (R10)
TR88	A támadó megváltoztathatja a kérelem metaadatait (szolgáltatás neve, felhasználás stb.).	Tranzakciómanipulálás (R10)
TR89	A támadó megváltoztathatja a válaszinformációkat (szolgáltatás állapota, egyszeri kulcs stb.).	Tranzakciómanipulálás (R10)
TR90	A támadó megváltoztathatja a kérelem attribútuminformációit (túl sok lekérdezés stb.).	Tranzakciómanipulálás (R10)
TR91	Az igénybe vevő fél az előző munkamenetből származó elemeket játszhat vissza egy másik munkamenetben.	Tranzakciómanipulálás (R10)
TR92	A támadó kicserélheti vagy módosíthatja a személyazonosító adatot a személyazonosítóadat-szolgáltatótól az adattárcaegységre való átvitele során.	Tranzakciómanipulálás (R10)
TR93	A támadó kicserélheti vagy módosíthatja a személyazonosító adatot az adattárcaegységről az online igénybe vevő félhez való átvitele során.	Tranzakciómanipulálás (R10)
TR94	A támadó kicserélheti vagy módosíthatja a személyazonosító adatot az adattárcaegységről az offline igénybe vevő félhez való átvitele során.	Tranzakciómanipulálás (R10)
TR95	A támadó a felhasználó hozzájárulása nélkül is kiállíthat személyazonosító adatokat.	Nem engedélyezett tranzakció (R9)
TR96	A támadó visszavont vagy érvénytelen beágyazott közzétételi szabályzatokat alkalmazhat, akár az igénybe vevő felek tudta nélkül.	Nem engedélyezett tranzakció (R9)
TR97	A támadó megtéveszti az adattárcát, hogy helytelen elektronikus aláírást ellenőrizzen.	Nem engedélyezett tranzakció (R9)
TR98	A támadó úgy is használhatja az adattárcát, hogy az nincs a felhasználó ellenőrzése alatt.	Nem engedélyezett tranzakció (R9)

Azonosító *Azonosító*	Veszélyforrás leírása *Az azonosított veszélyforrás ismertetése (*)*	Kockázat megnevezése *Kapcsolódó kockázatok*
TR99	A támadó ráveheti a felhasználót, hogy hitelesítse és hagyja jóvá a támadóval vagy illetéktelen harmadik féllel folytatott tranzakciókat.	Nem engedélyezett tranzakció (R9)
TR100	A támadó elektronikus aláírásra veheti rá a felhasználót anélkül, hogy megjelenítené neki a tartalmat, vagy azután, hogy helytelen tartalmat jelenített meg.	Nem engedélyezett tranzakció (R9)
TR101	A támadó megkerülheti a felhasználó adattárca-szolgáltatónál vezetett fiókjához való hozzáférés ellenőrzését.	Nem engedélyezett tranzakció (R9)
TR102	A támadó az igénybe vevő felekhez való csatlakozás során visszaélhet az igénybe vevő felek személyazonosságával.	Nem engedélyezett tranzakció (R9)/ adatok közzététele (R6)
TR103	Az igénybe vevő fél és a böngésző közötti kapcsolat hátterében álló felhasználó különbözhet az igénybe vevő fél és az adattárca közötti kapcsolat mögötti felhasználótól.	Nem engedélyezett tranzakció (R9)/ adatok közzététele (R6)/ személyazonosság-lopás (R4)
TR104	A támadó meggyőzheti a felhasználót, hogy ok nélkül visszavonja a felhasználó adattárcáját.	Nem engedélyezett tranzakció (R9)/ szolgáltatás zavara (R13)
TR105	A támadó közbeékelődéses támadást hajthat végre.	Nem engedélyezett tranzakció (R9)/ adatok közzététele (R6)/megfigyelés (R14)
TR106	A támadó olyan adattárcából jeleníthet meg érvénytelen vagy visszavont attribútumokat, amely nem csatlakozik rendszeresen a hálózathoz.	Különféle kockázatokra kifejtett hatás
TR107	A támadó adattárca hamisításával információkat tulajdoníthat el a felhasználótól.	Különféle kockázatokra kifejtett hatás
TR108	A támadó adatkérelem (pl. hitelesítés) érvényesnek tűnő visszajátszása/utánzása révén visszaélhet a felhasználó személyazonosságával.	Különféle kockázatokra kifejtett hatás
TR109	A támadó beágyazott közzétételi szabályzatot játszhat vissza a felhasználónak egy jóváhagyott kérelem utánzásához.	Különféle kockázatokra kifejtett hatás
TR110	A támadó a biztonság megsértése vagy veszélyeztetése után kihasználhatja az adattárca-felhasználók információhiányát vagy az indokolatlan késedelmeket.	Különféle kockázatokra kifejtett hatás
TR111	A támadó rosszindulatú funkciók hozzáadása érdekében módosíthatja a korábban telepített legitim adattárcapéldányt.	Különféle kockázatokra kifejtett hatás
TR112	A támadó módosíthatja a legitim adattárcapéldányt, és a felhasználóknak legitimként ajánlhatja fel.	Különféle kockázatokra kifejtett hatás
TR113	A támadó kijátszhatja a felhasználóhitelesítési mechanizmust, hogy megkerülje az adattárca-felhasználó hitelesség-ellenőrzését.	Különféle kockázatokra kifejtett hatás
TR114	A támadó kártékony kódot vagy hátsó ajtót illeszthet be az adattárcakódba annak felhasználói eszközre történő telepítése során.	Különféle kockázatokra kifejtett hatás
TR115	A támadó kártékony kódot vagy hátsó ajtót illeszthet be az adattárcakódba annak fejlesztése során.	Különféle kockázatokra kifejtett hatás
TR116	A támadó illetéktelenül módosíthatja a véletlenszerű számok generálását, hogy kellőképpen csökkentse az entrópiájukat a támadások lehetővé tételéhez.	Különféle kockázatokra kifejtett hatás

Azonosító *Azonosító*	Veszélyforrás leírása *Az azonosított veszélyforrás ismertetése (*)*	Kockázat megnevezése *Kapcsolódó kockázatok*
TR117	A támadó illetéktelenül módosíthatja a felhasználói eszközöket az ellátási láncban, hogy olyan kódokat vagy konfigurációkat tartalmazzanak, amelyek nem felelnek meg az adattárca használati feltételeinek.	Különféle kockázatokra kifejtett hatás
TR118	A támadó az általa irányított, hamisított adattárca-biztonsági kriptográfiai eszköz használatával aktiválhatja az adattárcaegységet.	Különféle kockázatokra kifejtett hatás
TR119	A támadó elolvashatja az adattárca-biztonsági kriptográfiai alkalmazásnak, illetve az adattárca-biztonsági kriptográfiai eszköznek küldött információkat.	Különféle kockázatokra kifejtett hatás
TR120	A támadó tetszőleges információkat küldhet az adattárca-biztonsági kriptográfiai alkalmazásnak.	Különféle kockázatokra kifejtett hatás
TR121	A támadó az adattárca-biztonsági kriptográfiai alkalmazás és az adattárca-biztonsági kriptográfiai eszköz közötti információcsere lehallgatásával információkat lophat.	Különféle kockázatokra kifejtett hatás
TR122	A támadó tetszőleges információkat küldhet az adattárca-biztonsági kriptográfiai eszköznek.	Különféle kockázatokra kifejtett hatás
TR123	A támadó az adattárca-biztonsági kriptográfiai alkalmazást megkerülve küldhet információkat az adattárca-biztonsági kriptográfiai eszköznek.	Különféle kockázatokra kifejtett hatás
TR124	A támadó adathalászat alkalmazásával hamis adattárcához és személyazonosítóadat-kezelő webalkalmazáshoz irányíthatja át a felhasználókat.	Különféle kockázatokra kifejtett hatás
TR125	A támadó az adattárca kulcsait más kulcsokkal helyettesítheti azért, hogy más támadás során használható üzeneteket hozzon létre.	Különféle kockázatokra kifejtett hatás
TR126	A támadó módosíthatja vagy megsemmisítheti az adattárca kulcsait, használhatatlanná téve az adattárca egyes funkcióit.	Különféle kockázatokra kifejtett hatás
TR127	A támadó kártékony szoftvereket irányítva hozzáférhet az adattárcában tárolt adatokhoz.	Különféle kockázatokra kifejtett hatás
TR128	A támadó hozzáférhet az adattárcában létrehozott tanúsító adatokhoz.	Különféle kockázatokra kifejtett hatás
TR129	Az adattárca-szolgáltatók hozzáférhetnek az adattárcában található objektumokhoz.	Különféle kockázatokra kifejtett hatás
TR130	Az adattárca-szolgáltatók hozzáférhetnek az adattárcában létrehozott tanúsító adatokhoz.	Különféle kockázatokra kifejtett hatás
TR131	A támadó ellophatja a feloldott adattárcaeszközöket.	Különféle kockázatokra kifejtett hatás
TR132	A támadó manipulálhatja a rendszert, hogy megakadályozza bizonyos események naplózását.	Különféle kockázatokra kifejtett hatás
TR133	A támadó lehallgathatja az adattárcapéldány és az adattárca-biztonsági kriptográfiai alkalmazás közötti kommunikációt, vagy visszajátszhatja/utánozhatja a felhasználót (például a hitelesítési mechanizmus eltérítésével).	Különféle kockázatokra kifejtett hatás

II. MELLÉKLET

A MEGBÍZHATÓSÁGI INFORMÁCIÓK ELFOGADHATÓSÁGÁNAK ÉRTÉKELÉSÉRE VONATKOZÓ KRITÉRIUMOK

Név	Tárgy	Fontos szempontok
EUCC	IKT-termékek	A kibocsátóval kapcsolatban: nincs (akkreditált tanúsító szervek) A hatókörrel kapcsolatban: — A védelmi profil és a biztonsági előirányzat ellenőrzése — Az értékelési biztonsági szint és a kiterjesztések ellenőrzése A megbízhatósággal kapcsolatban: — A felhasználói dokumentációban szereplő korlátozások ellenőrzése — Az összetételt illetően az értékelési technikai jelentéshez való hozzáférésre lehet szükség
EUCS (amennyiben rendelkezésre áll)	Felhőszolgáltatások	A kibocsátóval kapcsolatban: nincs (akkreditált tanúsító szervek) A hatókörrel kapcsolatban: — A felhőszolgáltatás leírásának ellenőrzése — Az értékelési szint és a tartozékprofilok ellenőrzése A megbízhatósággal kapcsolatban: — Az átláthatósági információk és szükség esetén az összetételre vonatkozó információk ellenőrzése
Az EU-ban működő közös kritériumrendszerek, beleértve a SOG-IS rendszereket is	IKT-termékek	A kibocsátóval kapcsolatban: nincs (tagállamok) A hatókörrel kapcsolatban: — A védelmi profil és a biztonsági előirányzat ellenőrzése — Az értékelési biztonsági szint és a kiterjesztések ellenőrzése A megbízhatósággal kapcsolatban: — A felhasználói dokumentációban szereplő korlátozások ellenőrzése — Az összetételt illetően az értékelési technikai jelentéshez való hozzáférésre lehet szükség
EN 17640:2018 (FITCEM, beleértve a CSPN, BSZ, LINCE, BSZA rendszereket)	IKT-termékek	A kibocsátóval kapcsolatban: — A rendszer és a tanúsító szervekre vonatkozó követelmények ellenőrzése A hatókörrel kapcsolatban: — A termékleírás ellenőrzése — A biztonságra vonatkozó állítások ellenőrzése — A biztonsági szint ellenőrzése A megbízhatósággal kapcsolatban: — Az elvégzett tevékenységek és a jelentésben szereplő megállapítások ellenőrzése
A 910/2014/EU rendelet 30. cikke szerinti minősített aláírást létrehozó eszközök tanúsítási rendszerei	QSCD	A kibocsátóval kapcsolatban: — A rendszer és a tanúsító szervekre vonatkozó követelmények ellenőrzése A hatókörrel kapcsolatban: — A termékleírás ellenőrzése — A biztonságra vonatkozó állítások ellenőrzése — A biztonsági szint ellenőrzése A megbízhatósággal kapcsolatban: — Az elvégzett tevékenységek ellenőrzése

Név	Tárgy	Fontos szempontok
EN ISO/IEC 27001:2022	ISMS	A kibocsátóval kapcsolatban: nincs (akkreditált tanúsító szervek) A hatókörrel kapcsolatban: — Az irányítási rendszer leírásának ellenőrzése — Az alkalmazhatósági nyilatkozat ellenőrzése A megbízhatósággal kapcsolatban: — Az elvégzett tevékenységek ellenőrzése
SOC2	Szervezetek	A kibocsátóval kapcsolatban: — Könyvvizsgálói státusz ellenőrzése A hatókörrel kapcsolatban: — A vezetőségi nyilatkozat és az ellenőrzések leírásának ellenőrzése — Az alkalmazhatósági nyilatkozat ellenőrzése A megbízhatósággal kapcsolatban: — A jelentés megállapításainak ellenőrzése — Szükség esetén az áthidaló levelek ellenőrzése
MDSCert (GSMA) (ha rendelkezésre áll)	Mobil eszközök	A kibocsátóval kapcsolatban: — A tanúsító szervekre vonatkozó követelmények ellenőrzése A hatókörrel kapcsolatban: — A biztonságigarancia-szint ellenőrzése — A rendszer követelményeinek ellenőrzése A megbízhatósággal kapcsolatban: — A jelentésben szereplő tevékenységek és megállapítások ellenőrzése
Egyéb rendszerek	Bármely összetevő	A rendszerrel kapcsolatban: — A rendszer relevanciájának és rendelkezéseinek ellenőrzése A kibocsátóval kapcsolatban: — A tanúsító szervekre vonatkozó követelmények ellenőrzése A hatókörrel kapcsolatban: — A rendszer követelményeinek ellenőrzése — A biztonsági előirányzat vagy a biztonsági funkcionális követelményeket és a biztonsági garanciára vonatkozó követelményeket leíró hasonló dokumentum ellenőrzése — A termékleírás és a kiválasztott biztonsági funkcionális követelmények ellenőrzése A megbízhatósággal kapcsolatban: — A jelentésben szereplő tevékenységek és megállapítások ellenőrzése

III. MELLÉKLET

AZ ADATTÁRCA-MEGOLDÁSOKRA VONATKOZÓ FUNKCIONÁLIS KÖVETELMÉNYEK

A 910/2014/EU rendelet 5a. cikkének (4), (5), (8) és (14) bekezdése értelmében a tanúsított adattárca-megoldás és a megoldást szolgáltató elektronikus azonosítási rendszer által teljesítendő funkcionális kritériumok közé kell tartozniuk a következőkben felsorolt tevékenységekre vonatkozó funkcionális követelményeknek:

1. a Bizottság (EU) 2024/2979 végrehajtási rendelete ([1]) a 910/2014/EU európai parlamenti és tanácsi rendeletnek az integritás és alapvető funkciók tekintetében történő alkalmazására vonatkozó szabályok megállapításáról;
2. a Bizottság (EU) 2024/2982 végrehajtási rendelete ([2]) a 910/2014/EU európai parlamenti és tanácsi rendeletnek az európai digitális személyazonossági keret által támogatandó protokollok és interfészek tekintetében történő alkalmazására vonatkozó szabályok megállapításáról;
3. a Bizottság (EU) 2024/2977 végrehajtási rendelete ([3]) a 910/2014/EU európai parlamenti és tanácsi rendeletnek az európai digitális személyiadat-tárcák részére kibocsátott személyazonosító adatok és elektronikus attribútumtanúsítványok tekintetében történő alkalmazására vonatkozó szabályok megállapításáról.

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

([2]) A Bizottság (EU) 2024/2982 végrehajtási rendelete (2024. november 28.) a 910/2014/EU európai parlamenti és tanácsi rendeletnek az európai digitális személyazonossági keret által támogatandó protokollok és interfészek tekintetében történő alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/2982, 2024.12.4., ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) A Bizottság (EU) 2024/2977 végrehajtási rendelete (2024. november 28.) a 910/2014/EU európai parlamenti és tanácsi rendeletnek az európai digitális személyiadat-tárcák részére kibocsátott személyazonosító adatok és elektronikus attribútumtanúsítványok tekintetében történő alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/2977, 2024.12.4., ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

IV. MELLÉKLET

AZ ÉRTÉKELÉSI TEVÉKENYSÉGEK ELVÉGZÉSÉNEK MÓDSZEREI ÉS ELJÁRÁSAI

1. **Az adattárca-megoldások megvalósításának ellenőrzése**

A megfelelőségértékelési tevékenység része az egyedi értékelési tevékenységek kiválasztása.

A nemzeti tanúsítási rendszerek meghatározzák a szolgáltatott információk értékelésére szolgáló tevékenységet, amely legalább a következőkre terjed ki:

a) a szolgáltatott információk elemzése annak megerősítéséhez, hogy azok alkalmasak a nemzeti tanúsítási rendszerekben meghatározott architektúrák valamelyikében való használatra;

b) az I. melléklet szerinti kockázat-nyilvántartásban azonosított kiberbiztonsági kockázatok és veszélyforrások ismertetett biztonsági ellenőrzésekkel való fedezésének elemzése.

Az a)–b) pontban említett elemzésnek az adattárca szolgáltatója által adott magyarázaton és indokoláson kell alapulnia.

2. **Az adattárca-biztonsági kriptográfiai eszközzel (WSCD) kapcsolatos értékelési tevékenységek**

(1) A kritikus műveleteket – a kriptográfiai számításokat is beleértve – nem szükséges teljes mértékben végrehajtani a WSCD-ben. A WSCD-ben végrehajtott rész azonban az (EU) 2015/1502 bizottsági végrehajtási rendelettel [1] összhangban garantálja az általa végzett kritikus műveletek védelmét a nagy támadási potenciálú támadókkal szemben, amennyiben a WSCD az adattárca-megoldás részeként működik.

(2) A WSCD vagy annak egy része képezheti tanúsítás tárgyát, ha azt a tanúsítvány jogosultja vagy a tanúsítást kérelmező biztosítja, vagy lehet annak hatókörén kívül, ha a végfelhasználó által biztosított eszközbe van beágyazva. Emellett a nemzeti tanúsítási rendszereknek a következő két esetben meghatározzák a WSCD megfelelőségének ellenőrzésére irányuló értékelési tevékenységeket:

a) ha az adattárca-biztonsági kriptográfiai alkalmazás (WSCA) az adott WSCD-től függ (azaz a WSCD alapján összetett termékként kell értékelni), akkor a WSCA értékelése céljából hozzáférést kell biztosítani a WSCD tanúsításával kapcsolatos további információkhoz, beleértve különösen az értékelési technikai jelentést;

b) ha a rendszerben figyelembe vett architektúra több WSCD-t használ, vagy ha a kritikus eszközökkel kapcsolatos egyes műveleteket a WSCD-n kívül végzik, a nemzeti tanúsítási rendszerek értékelési tevékenységeket tartalmaznak annak biztosítása érdekében, hogy az átfogó megoldás az elvárt biztonsági szintet nyújtsa.

(3) A nemzeti tanúsítási rendszerek szerinti tanúsítás előfeltételeként a WSCD-t az (EU) 2015/1502 végrehajtási rendeletben meghatározott „magas” biztonsági szintre vonatkozó követelmények alapján kell értékelni.

a) Amennyiben teljesülnek a 3. cikk (3) bekezdésének b) pontjában foglalt feltételek, a WSCD vagy annak egy része értékelésének részét képezi az (EU) 2024/482 bizottsági végrehajtási rendelet [2] I. mellékletében foglalt AVA_VAN 5. szintű, az EN ISO/IEC 15408-3:2022 szabványban meghatározott sebezhetőségi értékelés, kivéve, ha a tanúsító szervnek kellőképpen indokolják, hogy a WSCA biztonsági jellemzői lehetővé teszik alacsonyabb értékelési szint alkalmazását, miközben az (EU) 2015/1502 végrehajtási rendeletben meghatározott általános biztonsági szint „magas” marad.

[1] A Bizottság (EU) 2015/1502 végrehajtási rendelete (2015. szeptember 8.) az elektronikus azonosító eszközök biztonsági szintjeire vonatkozó minimális technikai specifikációknak és eljárásoknak a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 8. cikkének (3) bekezdése szerint történő megállapításáról (HL L 235., 2015.9.9., 7. o., ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

[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/oj).

(4) Emellett az egyes konkrét architektúrákra vonatkozó dokumentációban a nemzeti tanúsítási rendszerek a WSCD ezen értékeléséhez olyan feltételezéseket fogalmaznak meg, amelyek alapján az (EU) 2015/1502 végrehajtási rendelettel összhangban biztosítható a nagy támadási potenciálú támadókkal szembeni ellenállás, és meghatározzák az e feltételezéseknek és a tanúsítvány kiállítását követően annak megerősítésére irányuló értékelési tevékenységeket, hogy a feltételezések továbbra is ellenőrzöttek. A nemzeti rendszerek arra is kötelezik a tanúsításra pályázókat, hogy pontosítsák ezeket a feltételezéseket azok konkrét végrehajtása tekintetében, és ismertessék azokat az intézkedéseket, amelyek garantálják, hogy a feltételezéseket a tanúsítás teljes életciklusa során ellenőrzik.

(5) A nemzeti tanúsítási rendszereknek minden esetben részük az annak ellenőrzését szolgáló értékelési tevékenység, hogy a WSCD rendelkezésére álló megbízhatósági információk megfelelőek-e az adattárca-megoldás céljára, a megbízhatósági információk – például az EUCC-tanúsítványokra vonatkozó biztonsági előirányzat – elemzése révén, beleértve a következő tevékenységeket:

a) annak ellenőrzése, hogy az értékelés hatóköre megfelelő-e, ami az EUCC-tanúsítványok esetében például annak ellenőrzését jelenti, hogy a biztonsági előirányzat megfelel-e az EUCC-ben ajánlott védelmi profilok egyikének;

b) annak ellenőrzése, hogy a működési környezetre vonatkozó feltételezések összeegyeztethetők-e az adattárca-megoldással, ami például az EUCC-tanúsítványok esetében azt jelenti, hogy ezek a feltételezések megtalálhatók a biztonsági előirányzatban;

c) annak ellenőrzése, hogy a felhasználói útmutatóban vagy dokumentációban foglalt ajánlások összeegyeztethetők-e azokkal a feltételekkel, amelyek mellett a WSCD-t az adattárca-megoldásban használni kell;

d) annak ellenőrzése, hogy a nemzeti tanúsítási rendszerben a WSCD-kre vonatkozóan tett feltételezéseket ellenőrizték-e, és azok szerepelnek-e a megbízhatósági információkban.

(6) Azokban az esetekben, amikor egyes ellenőrzések nem teljes mértékben meggyőzőek, a nemzeti tanúsítási rendszerek előírják a tanúsító szervek számára, hogy a WSCD alapján határozzák meg a WSCA-ra vonatkozó kompenzációs követelményeket, amelyekre ki kell terjednie a WSCA értékelésének. Ha ez nem lehetséges, a nemzeti tanúsítási rendszerek a WSCD-t nem megfelelőnek tekintik, ami azt jelenti, hogy az adattárca-megoldáshoz nem állítható ki megfelelőségi tanúsítvány.

3. **Az adattárca-biztonsági kriptográfiai alkalmazással (WSCA) kapcsolatos értékelési tevékenységek**

(1) A nemzeti tanúsítási rendszerek előírják, hogy a WSCA-t az adattárca-megoldás részeként legalább az (EU) 2015/1502 végrehajtási rendeletben meghatározott „magas” biztonsági szintre vonatkozó követelmények alapján értékeljék.

(2) Ennek az értékelésnek a részét képezi az (EU) 2024/482 végrehajtási rendelet I. mellékletében foglalt AVA_VAN 5. szintű, az EN ISO/IEC 15408-3:2022 szabványban meghatározott sebezhetőségi értékelés, kivéve, ha a tanúsító szervnek kellőképpen indokolják, hogy a WSCA biztonsági jellemzői lehetővé teszik alacsonyabb értékelési szint alkalmazását, miközben az (EU) 2015/1502 végrehajtási rendeletben meghatározott általános biztonsági szint magas marad.

(3) Amennyiben a WSCA-t nem az adattárca-szolgáltató biztosítja, a nemzeti tanúsítási rendszerek a WSCA ezen értékeléséhez olyan feltételezéseket fogalmaznak meg, amelyek alapján az (EU) 2015/1502 végrehajtási rendelettel összhangban biztosítható a nagy támadási potenciálú támadókkal szembeni ellenállás, és meghatározzák az e feltételezéseknek és a tanúsítvány kiállítását követően annak megerősítésére irányuló értékelési tevékenységeket, hogy a feltételezések továbbra is ellenőrzöttek. A nemzeti rendszerek arra is kötelezik a tanúsításra pályázókat, hogy pontosítsák ezeket a feltételezéseket azok konkrét végrehajtása tekintetében, és ismertessék azokat az intézkedéseket, amelyek garantálják, hogy a feltételezéseket a tanúsítás teljes életciklusa során ellenőrzik.

(4) A nemzeti tanúsítási rendszereknek minden esetben részük az annak ellenőrzését szolgáló értékelési tevékenység, hogy a WSCA rendelkezésére álló megbízhatósági információk megfelelőek-e az adattárca-megoldás céljára, a megbízhatósági információk – például az EUCC-tanúsítványokra vonatkozó biztonsági előirányzat – elemzése révén, beleértve a következő tevékenységeket:

a) annak ellenőrzése, hogy az értékelés hatóköre megfelelő-e, ami az EUCC-tanúsítványok esetében például annak ellenőrzését jelenti, hogy a biztonsági előirányzat megfelel-e az EUCC-ben ajánlott védelmi profilok egyikének;

b) annak ellenőrzése, hogy a működési környezetre vonatkozó feltételezések összeegyeztethetők-e az adattárca-megoldással, ami például az EUCC-tanúsítványok esetében azt jelenti, hogy ezek a feltételezések megtalálhatók a biztonsági előirányzatban;

c) annak ellenőrzése, hogy a felhasználói útmutatóban vagy dokumentációban foglalt ajánlások összeegyeztethetők-e azokkal a feltételekkel, amelyek mellett a WSCA-t az adattárca-megoldásban használni kell;

d) annak ellenőrzése, hogy a nemzeti tanúsítási rendszerben a WSCA-kra vonatkozóan tett feltételezéseket ellenőrizték-e, és azok szerepelnek-e a megbízhatósági információkban.

(5) A nemzeti tanúsítási rendszerek előírják, hogy a WSCA értékelése az ezen WSCA által végrehajtott összes biztonsági ellenőrzésre kiterjedjen.

4. **A végfelhasználói eszközzel kapcsolatos értékelési tevékenységek**

Mivel az e rendelet I. mellékletében meghatározott kockázat-nyilvántartás olyan kockázatokat határoz meg, amelyek közvetlenül kötődnek a végfelhasználói eszköz biztonságához, a nemzeti tanúsítási rendszerek meghatározzák a végfelhasználói eszközökre vonatkozó biztonsági követelményeket. Mivel azonban ezeket az eszközöket a végfelhasználó, nem pedig az adattárca-szolgáltató biztosítja, ezekre a követelményekre feltételezések vonatkoznak.

Az adattárca-megoldásnak minden feltételezés esetében tartalmaznia kell egy olyan mechanizmust, amely minden adattárcaegység esetében ellenőrzi, hogy a mögöttes végfelhasználói eszköz megfelel-e a feltételezésnek. Ezek a mechanizmusok biztonsági ellenőrzéseknek minősülnek, és kiterjednek rájuk az értékelési tevékenységek, hogy a megfelelő biztonsági szinten igazolják megfelelőségüket és eredményességüket.

Az alábbiakban két szemléltető példa olvasható:

a) A végfelhasználói eszköz tartalmazhat tanúsított WSCD-t, amelynek tanúsítását igazolni kell. Ehhez jellemzően kriptográfiai mechanizmus alkalmazásával ellenőriznék, hogy a tanúsított WSCD-ben van-e olyan kriptográfiai titkos kulcs, amely csak a tanúsított WSCD-ben áll rendelkezésre. Ez esetben a szóban forgó kriptográfiai titkos kulcsot kritikus eszköznek kell tekinteni, és ki kell terjednie rá a WSCD, illetve a WSCA tanúsításának.

b) A végfelhasználói eszközökre vonatkozó jellemző követelmény az lenne, hogy az eszközöknek biztonsági frissítéseket kell kapniuk. Mivel ez a követelmény az adattárcapéldányhoz kapcsolódik, a biztonsági frissítések rendelkezésre állásának ellenőrzésére alkalmazott mechanizmusra csak az adattárcapéldánynak megfelelő biztonsági szintű értékelési tevékenységeknek szükséges kiterjedniük, különösen azért, mert a mechanizmus valószínűleg az adattárcapéldány szerves része lesz.

5. **Az adattárcapéldánnyal kapcsolatos értékelési tevékenységek**

(1) Az adattárcapéldány értékelése során a következő két fő kihívást kell figyelembe venni:

a) az adattárcapéldány valószínűleg ugyanazon alapalkalmazás több változatában is létezik, és minden egyes változat a végfelhasználói eszközök adott kategóriájára specializálódott;

b) az adattárcapéldány különböző változatait valószínűleg gyakran frissíteni kell, hogy lépést tartson a mögöttes biztonsági platform fejlesztésével – például ha olyan sebezhetőségeket azonosítanak, amelyek miatt módosítani kell az alkalmazásokat.

(2) Az adattárcapéldány értékelése során figyelembe kell venni az említett sajátos kihívásokat. Ennek egyik közvetlen következménye az, hogy a közös kritériumok rendszere nem minden esetben alkalmazható, ezért szükség esetén alternatív értékelési módszereket kell fontolóra venni. A nemzeti tanúsítási rendszereknek mérlegelniük kell az EN 17640:2018 szabvány módszertanának alkalmazását a következők szerint:

a) magának a rendszernek a részeként;

b) a módszertanon alapuló nemzeti rendszerek révén;

c) hasonló elveken alapuló, de az EN 17640:2018 módszertanának kidolgozása előtt létrehozott nemzeti rendszerek révén.

(3) Emellett, mivel az egyes változatok teljeskörű célzott értékelésének elvégzése csak korlátozott hozzáadott értékkel bírhat, a nemzeti tanúsítási rendszereknek mérlegelniük kell a mintavétel elvégzését lehetővé tevő kritériumok meghatározását azért, hogy elkerülhető legyen az azonos értékelési tevékenységek megismétlése, és hogy az adott változatra jellemző tevékenységekre összpontosítsanak. A nemzeti tanúsítási rendszerek előírják minden tanúsító szerv számára, hogy indokolják az általuk alkalmazott mintavételt.

(4) A nemzeti tanúsítási rendszerek az adattárcapéldány frissítéseit is beleveszik az adattárcamegoldáshoz meghatározott átfogó változáskezelési folyamatba. Szabályokat állapítanak meg továbbá az adattárca-szolgáltató által minden frissítés esetében elvégzendő eljárásokra (pl. a változások biztonsági ellenőrzésekre gyakorolt hatásának elemzése), valamint a tanúsító szerv által a frissítéseken meghatározott feltételek mellett elvégzendő értékelési tevékenységekre (pl. a módosított biztonsági ellenőrzések operatív eredményességének értékelése). A változáskezelési folyamat az egyik olyan folyamat, amelynek eredményes működését a 18. cikk (3) bekezdésével összhangban évente ellenőrizni kell.

6. **Az adattárca-megoldás biztosításához és működtetéséhez használt szolgáltatásokkal és folyamatokkal kapcsolatos értékelési tevékenységek**

(1) Az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszer biztosításában és működtetésében szerepet játszó szolgáltatások és folyamatok értékeléséhez az értékelő csoportnak bizonyítékokat kell gyűjtenie. Az erre szolgáló értékelési tevékenység lehet többek között ellenőrzés, helyszíni szemle, felülvizsgálat és érvényesítés.

(2) A tanúsító szerv megerősíti, hogy a bizonyítékok elégségesek és megfelelőek ahhoz, hogy elegendő biztosítékot nyújtsanak arra, hogy a szolgáltatások és az eljárások megfelelnek a tanúsítási követelményeknek. Ennek keretében megerősíti:

a) a folyamatok és szolgáltatások leírásában szereplő információk helytállóságát;

b) a folyamatok és szolgáltatások tervezésének és ellenőrzésének alkalmasságát arra, hogy megfeleljen az értékelési feltételeknek;

c) a szóban forgó ellenőrzések végrehajtásának operatív eredményességét az értékelést megelőző meghatározott időszakban.

(3) A leírás helytállósága és az ellenőrzések végrehajtásának operatív eredményessége az adattárca-szolgáltató megfelelő állításaira vonatkozó – az ISO/IEC 17000:2020 szabvány értelmezésében vett – ellenőrzési célkitűzésnek tekinthető (azaz a már bekövetkezett események vagy elért eredmények helytállóságának megerősítése), míg a szolgáltatások és folyamatok tervezésének és ellenőrzésének az értékelési feltételeknek való megfelelésre való alkalmassága az adattárca-szolgáltató megfelelő állítására – az ISO/IEC 17000:2020 értelmezésében vett – érvényesítési célkitűzésnek tekinthető (azaz a tervezett jövőbeli felhasználásra vagy az előre jelzett eredményre vonatkozó hitelesség megerősítése).

(4) Tekintettel arra, hogy az adattárca-megoldások tanúsítás nélkül nem működhetnek, az eredményes működés nem erősíthető meg a megoldás tényleges működése alapján. Ezért ezt vizsgálatok vagy kísérleti bevezetés során gyűjtött bizonyítékok felhasználásával igazolják.

(5) Előfordulhat, hogy már léteznek nemzeti tanúsítási rendszerek bizonyos szolgáltatásokra és folyamatokra, például a felhasználók beléptetésére. Az ilyen rendszerek alkalmazását adott esetben mérlegelik a nemzeti tanúsítási rendszerek.

7. **Az adattárca-megoldás biztosításához és működtetéséhez használt IKT-szolgáltatásokkal kapcsolatos értékelési tevékenységek**

(1) Egyes adattárca-architektúrák célzott IKT-szolgáltatásokra támaszkodhatnak – többek között az adattárca-megoldás biztosításához és működtetéséhez szükséges felhőszolgáltatásokra –, amelyek érzékeny adatokat tárolhatnak, valamint érzékeny műveleteket tehetnek lehetővé. Ilyen esetben a nemzeti tanúsítási rendszerek meghatározzák a szóban forgó IKT-szolgáltatásokra sajátos biztonsági követelményeit.

(2) Már számos tanúsítási rendszer létezik az IKT-szolgáltatásokhoz, a felhőszolgáltatásokhoz és más megbízhatósági információforrásokhoz, beleértve a II. mellékletben felsoroltakat is. Amennyiben rendelkezésre állnak és alkalmazhatók, az ilyen meglévő mechanizmusokra támaszkodnak a nemzeti tanúsítási rendszerek, az egyik alábbi mechanizmus révén:

a) kötelezővé teszik egy adott rendszer vagy több kiválasztott rendszer használatát azoknak a feltételeknek a meghatározásával, amelyek alapján az IKT- vagy felhőszolgáltatásokat a szóban forgó rendszerek felhasználásával értékelik;

b) az értékelés kiválasztását az adattárca-szolgáltatóra bízva a függőségi elemzési tevékenységet használják fel az értékelések során szerzett megbízhatósági információk adott célra való alkalmasságának elemzésére.

(3) A nemzeti tanúsítási rendszerek mindkét esetben meghatározzák az ezen rendszerek révén szerzett információk elemzéséhez vagy kiegészítéséhez szükséges további értékelési tevékenységeket.

V. MELLÉKLET

AZ ADATTÁRCÁKRA VONATKOZÓ, NYILVÁNOSAN HOZZÁFÉRHETŐ INFORMÁCIÓK JEGYZÉKE

1. A 8. cikk (5) bekezdése alapján nyilvánosságra hozandó információknak legalább a következőket kell tartalmazniuk:

   a) az adattárca-megoldás használatára vonatkozó korlátozások;

   b) a végfelhasználóknak az adattárcák biztonságos konfigurálásában, beszerelésében, telepítésében, üzemeltetésében és karbantartásában segítséget nyújtó adattárca-szolgáltatói iránymutatások és ajánlások;

   c) a végfelhasználóknak nyújtott biztonsági támogatás időtartama, különös tekintettel a kiberbiztonsághoz kapcsolódó frissítések rendelkezésre állására;

   d) a gyártó vagy a szolgáltató kapcsolattartási adatai, valamint a végfelhasználóktól vagy biztonsági kutatóktól érkező, sebezhetőséggel kapcsolatos információk fogadásának elfogadott módszerei;

   e) az adattárcákhoz kapcsolódó, nyilvánosságra hozott sebezhetőségeket tartalmazó online adatbankokra és a releváns kiberbiztonsági tanácsadókra mutató hivatkozások.

2. Az 1. bekezdésben említett információkat közérthetően, teljeskörűen és könnyen hozzáférhető formában, nyilvánosan elérhető helyen minden olyan személy rendelkezésére bocsátják, aki adattárca-megoldást kíván használni.

VI. MELLÉKLET

A MEGBÍZHATÓSÁGI INFORMÁCIÓK ELFOGADHATÓSÁGÁNAK ÉRTÉKELÉSÉRE SZOLGÁLÓ MÓDSZERTAN

1. A megbízhatósági dokumentáció rendelkezésre állásának értékelése

Az értékelők felsorolják az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszer minden releváns összetevőjéről rendelkezésre álló megbízhatósági dokumentációt. Ezután az értékelők felmérik az egyes megbízhatósági dokumentumok általános relevanciáját a függőségi felülvizsgálat szempontjából.

Az elemzés során a következő szempontokat veszik figyelembe:

1. magáról a megbízhatósági dokumentációról:

   a) a megbízhatósági dokumentáció típusa, az összes előírt adattal együtt

      (ilyen dokumentum például az EN ISO/IEC 27001:2022 szabvány szerinti megfelelőségi nyilatkozat, vagy az 1-es vagy 2-es típusú ISAE-jelentések);

   b) a tárgyidőszak vagy az érvényességi idő

      (ez az időszak kiegészíthető áthidaló levéllel [az aktuális ISAE-jelentés adatszolgáltatási időszakának záró dátuma és az új ISAE-jelentés közzététele közötti időszakot lefedő dokumentummal] vagy hasonló nyilatkozattal);

   c) az alkalmazandó keret (pl. meglévő szabvány);

   d) a megbízhatósági dokumentáció tartalmazza-e a rendszer követelményeinek való megfeleltetést.

2. a megbízhatósági jelentés kibocsátójának szakmai kompetenciájáról és pártatlanságáról:

   a) a tanúsító szerv neve és – ha rendelkezésre áll – az értékelésvezető neve,

   b) a tanúsító szerv és az értékelő kompetenciájának igazolása (pl. akkreditáció, személyi tanúsítás stb.),

   c) a tanúsító szerv és az értékelő pártatlanságának igazolása (pl. akkreditáció stb.).

2. Az egyedi követelményekkel kapcsolatos megbízhatóság értékelése

Az értékelők ellenőrzik, hogy az adattárca-megoldásról és a megoldások szolgáltatására használt elektronikus azonosítási rendszerről rendelkezésre álló megbízhatósági dokumentáció megfelelő-e annak megállapításához, hogy az adattárca-megoldás megfelel a tanúsítási rendszer egyedi követelményeihez fűződő elvárásoknak.

Ezt az értékelést az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszer valamennyi releváns összetevőjére vonatkozóan elvégzik, az adattárca-megoldás biztonsági ellenőrzéseire vonatkozó feltevés megfogalmazásával.

Az értékelő csoport minden ilyen feltevés esetében meghatározza, hogy a rendelkezésre álló megbízhatósági dokumentációban biztosított megbízhatóság megfelelő-e.

Annak megállapítása, hogy a megbízhatóság megfelelő-e, a következőkön alapul:

1. a szükséges információk a várható biztonsági szinttel együtt rendelkezésre állnak a megbízhatósági dokumentációban;

2. a megbízhatósági dokumentációban rendelkezésre álló információk nem fedik le a követelmény teljes hatókörét, ám az adattárca-megoldásban vagy a megoldások szolgáltatására használt elektronikus azonosítási rendszerben megvalósított kiegészítő vagy helyettesítő ellenőrzések (azaz a meglévő vagy potenciális ellenőrzési hiányosságok kockázatát enyhítő belső kontrollmechanizmusok) lehetővé teszik az értékelők számára annak megállapítását, hogy az információk megfelelőek;

3. a megbízhatósági dokumentációban rendelkezésre álló információk nem adják meg a várt biztonsági szintet, de az adattárca-szolgáltató értékelése és figyelemmel kísérése érdekében végrehajtott ellenőrzések lehetővé teszik az értékelők számára annak megállapítását, hogy az információk megfelelőek;

4. ha a megbízhatósági dokumentáció meg nem feleléseket említ a feltevés teljesüléséhez használt ellenőrzések kialakítása vagy végrehajtása tekintetében, az adattárca-szolgáltató által javasolt és végrehajtott és az értékelők által felülvizsgált korrekciós intézkedéseknek megfelelőeknek kell lenniük, hogy garantálják a feltevés tényleges teljesülését.

VII. MELLÉKLET

A MEGFELELŐSÉGI TANÚSÍTVÁNY TARTALMA

1. A megfelelőségi tanúsítványt kiállító tanúsító szerv által hozzárendelt egyedi azonosító.

2. A tanúsított adattárca-megoldáshoz és a megoldások szolgáltatására használt elektronikus azonosítási rendszerekhez kapcsolódó, valamint a megfelelőségi tanúsítvány jogosultjára vonatkozó információk, többek között:
   a) az adattárca-megoldás neve;
   b) az adattárca-megoldás szolgáltatására használt elektronikus azonosítási rendszerek neve,
   c) az értékelt adattárca-megoldás verziója,
   d) a megfelelőségi tanúsítvány jogosultjának neve, címe és elérhetőségei,
   e) a megfelelőségi tanúsítvány jogosultjának a nyilvánosan hozzáférhetővé teendő információkat tartalmazó honlapjára mutató hivatkozás.

3. Az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszerek értékelésével és tanúsításával kapcsolatos információk, többek között:
   a) a megfelelőségi tanúsítványt kiállító tanúsító szerv neve, címe és elérhetőségei;
   b) amennyiben eltér a tanúsító szervtől, az értékelést végző megfelelőségértékelő szervezet neve, az akkreditálására vonatkozó információkkal együtt;
   c) a rendszertulajdonos neve;
   d) hivatkozások a 910/2014/EU rendeletre és erre a rendeletre;
   e) hivatkozás a megfelelőségi tanúsítványhoz kapcsolódó tanúsítási jelentésre;
   f) hivatkozás a megfelelőségi tanúsítványhoz kapcsolódó, tanúsításra vonatkozó értékelő jelentésre;
   g) hivatkozás az értékeléshez használt szabványokra, beleértve azok verzióit is;
   h) a megfelelőségi tanúsítvány kiállításának dátuma;
   i) a megfelelőségi tanúsítvány érvényességi ideje.

VIII. MELLÉKLET

A NYILVÁNOS TANÚSÍTÁSI JELENTÉS ÉS A TANÚSÍTÁSRA VONATKOZÓ ÉRTÉKELŐ JELENTÉS TARTALMA

1. A nyilvános tanúsítási jelentésnek legalább a következőket kell tartalmaznia:

   a) vezetői összefoglaló;

   b) az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszer meghatározása;

   c) az adattárca-megoldás és a megoldások szolgáltatására használt elektronikus azonosítási rendszer leírása;

   d) az V. mellékletben ismertetett, nyilvánosságra hozandó biztonsági információk vagy ezen információra mutató hivatkozás;

   e) az előzetes ellenőrzési és érvényesítési terv összefoglalója;

   f) a felülvizsgálat és a tanúsítási határozat összefoglalója.

2. A tanúsításra vonatkozó értékelő jelentésnek legalább a következőket kell tartalmaznia:

   a) az adattárca-megoldás kialakításának, az azonosítási rendszernek és a beléptetési folyamatnak a leírása, a kockázatértékeléssel és a konkrét érvényesítési tervvel együtt;

   b) annak leírása, hogy az adattárca-megoldás hogyan felel meg a „magas” biztonsági szintre vonatkozó követelményeknek, és hogy ezt hogyan igazolják az adattárca-megoldás e rendelettel összhangban végzett tanúsításértékelésének eredményei;

   c) az adattárca-megoldás és a megfelelő adattárcaegységeket biztosító elektronikus azonosítási rendszer megfelelőségértékelése eredményének ismertetése, különös tekintettel az alábbiaknak való megfelelésre:

      — a 910/2014/EU rendelet 5a. cikkének (4), (5), valamint (8) bekezdésében meghatározott követelmények,

      — a 910/2014/EU rendelet 5a. cikkének (14) bekezdésében meghatározott logikai elkülönítés követelménye,

      — adott esetben a 910/2014/EU rendelet 5a. cikkének (24) bekezdésében említett szabványok és technikai specifikációk, annak leírásával együtt, hogyan kapcsolódnak ezek a követelmények a nemzeti tanúsítási rendszerek által meghatározott megfelelő normatív követelményekhez.

   d) az érvényesítési terv elvégzése eredményének összefoglalója, beleértve minden feltárt meg nem felelést.

IX. MELLÉKLET

A KÖTELEZŐ FELÜGYELETI ÉRTÉKELÉSEK ÜTEMTERVE

1. A 18. cikk követelményeket határoz meg a tanúsítás életciklusára, különös tekintettel a rendszeres értékelési tevékenységek elvégzésére. Az említett tevékenységek legalább a következőket tartalmazzák:

   a) a megfelelőségértékelés tárgyának teljeskörű értékelése a kezdeti értékelés és minden újratanúsítási értékelés során, beleértve bármely termékkomponens frissítési funkcióját is;

   b) sebezhetőségi értékelés a kezdeti értékelés és minden újratanúsítási értékelés során, valamint legalább kétévente a felügyeleti értékelések során, amely kiterjed legalább a megfelelőségértékelés tárgyában és a fenyegetettségi környezetben a legutóbbi sebezhetőségi értékelés óta bekövetkezett változásokra;

   c) további tevékenységek, például behatolási tesztelés fokozott kockázati szint vagy új veszélyforrások megjelenése esetén;

   d) a karbantartási folyamatok eredményes működésének legalább évente történő értékelése a felügyeleti és újratanúsítási értékelések során, legalább a verziókövetési, frissítési és sebezhetőségkezelési folyamatokra kiterjedően;

   e) a sikeres felülvizsgálatot és tanúsítási határozatot követően megfelelőségi tanúsítvány kiállítása az első értékelés, majd minden újratanúsítási értékelés után.

2. Az 1. táblázat négyéves cikluson alapuló referencia-ütemtervet határoz meg, amelyben:

   a) az 1. év a megfelelőségi tanúsítvány első kiállításakor kezdődik; valamint

   b) minden értékelési tevékenységet az előző év értékelésétől számított 12 hónapon belül végeznek.

3. Az 1. táblázatban meghatározott ütemterv az időben történő újratanúsítás biztosítására és az adattárca-megoldás nyújtásában bekövetkező zavarok elkerülésére szóló ajánlás. Más ütemterv is lehetséges, feltéve, hogy a megfelelőségi tanúsítvány érvényessége nem haladja meg a 910/2014/EU rendelet 5c. cikkének (4) bekezdésében meghatározott öt évet.

4. A rendszeres értékelések mellett a tanúsító szervnek vagy a megfelelőségi tanúsítvány jogosultjának a kérésére különleges értékelés is indítható, miután jelentős változás következett be a tanúsítás tárgyában vagy a fenyegetettségi környezetben.

5. Minden értékelés – beleértve a felügyeleti értékeléseket és a különleges értékeléseket is – új megfelelőségi tanúsítvány kiállításához vezethet – különösen a tanúsítás tárgyának jelentős változása esetén –, ám a lejárat napja megegyezik az eredeti megfelelőségi tanúsítványéval.

1. táblázat

Teljes négyéves értékelési ciklus

Idő	Ért. típusa	Tevékenység
0. év	Kezdeti	— A tanúsítás tárgyának teljeskörű értékelése, beleértve a sebezhetőségi értékelést is — Minden egyes szoftverkomponens frissítésének elvégzésére szolgáló funkcióval — A karbantartási folyamatok értékelése, kivéve azok operatív eredményességét — A megfelelőségi tanúsítvány kiállítása és a négyéves ciklus kezdete
1. év	Felügyeleti	— A karbantartási folyamatok operatív eredményességének értékelése — Legalább verzió-ellenőrzés, frissítés, sebezhetőségkezelés — A termék biztonságára kiható változások értékelése

Idő	Ért. típusa	Tevékenység
2. év	Felügyeleti	— A teljes megoldás sebezhetőségi értékelése — A karbantartási folyamatok operatív eredményességének értékelése — Legalább verziókövetés, frissítés, sebezhetőségkezelés — A termék biztonságára kiható változások értékelése
3. év	Felügyeleti	— A karbantartási folyamatok operatív eredményességének értékelése — Legalább verzió-ellenőrzés, frissítés, sebezhetőségkezelés — A termék biztonságára kiható változások értékelése
4. év	Újratanúsítási	1. A tanúsítás tárgyának teljeskörű értékelése, beleértve a sebezhetőségi értékelést is 2. A változatlan jellemzők/folyamatok egyszerűsített értékelése 3. Minden egyes szoftverkomponens frissítésének elvégzésére szolgáló funkcióval 4. A karbantartási folyamatok értékelése, kitérve azok operatív eredményességére 5. Új megfelelőségi tanúsítvány kiállítása