2024/2979

2024.12.4.

A BIZOTTSÁG (EU) 2024/2979 VÉGREHAJTÁSI RENDELETE

(2024. november 28.)

a 910/2014/EU európai parlamenti és tanácsi rendeletnek az európai digitális személyiadat-tárcák integritása és alapvető funkciói tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

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 5a. cikke (23) bekezdésére,

mivel:

(1) A 910/2014/EU rendelettel létrehozott európai digitális személyazonossági keret kulcsfontosságú alapeleme a digitális személyazonosság Unió-szerte létrehozandó biztonságos és interoperábilis ökoszisztémájának. Az európai digitális személyiadat-tárcák (a továbbiakban: adattárcák) az egyik sarokkövét képezik ennek a keretnek, amelynek célja megkönnyíteni a természetes és jogi személyek számára a szolgáltatásokhoz való hozzáférést a tagállamokban, és egyúttal biztosítani a személyes adatok és a magánélet védelmét.

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

(3) A 910/2014/EU rendelet 5a. cikkének (23) bekezdése felhatalmazza a Bizottságot, hogy szükség esetén releváns specifikációkat és eljárásokat állapítson meg. E célból négy végrehajtási rendelet kerül elfogadásra, amelyek a protokollok és interfészek az (EU) 2024/2982 bizottsági végrehajtási rendelet ([4]), az integritás és az alapvető funkciók: az (EU) 2024/2979 bizottsági végrehajtási rendelet ([5]), a személyazonosító adatok és az elektronikus attribútumtanúsítványok az (EU) 2024/2977 bizottsági végrehajtási rendelet ([6]), illetve a Bizottságnak küldendő bejelentések az (EU) 2024/2980 bizottsági végrehajtási rendelet ([7]) aspektusait szabályozzák. Ez a rendelet az európai digitális személyiadat-tárcák integritására és alapvető funkcióira vonatkozó követelményeket határozza meg.

([1]) HL L 257., 2014.8.28., 73. o., ELI: https://eur-lex.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]) 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).

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

([6]) 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).

([7]) A Bizottság (EU) 2024/2980 végrehajtási rendelete (2024. november 28.) a 910/2014/EU európai parlamenti és tanácsi rendeletnek az európai digitális személyiadat-tárcák ökoszisztémájával kapcsolatban a Bizottságnak küldendő bejelentések tekintetében történő alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/2980, 2024.12.4., ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) 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 ([8]) nyomán elvégzett munkára támaszkodnak, különösen az architektúra és a referenciakeret tekintetében. Az (EU) 2024/1183 európai parlamenti és tanácsi rendelet ([9]) (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.

(5) A pontos kommunikáció, a műszaki különbségtétel, valamint a felelősségi körök egyértelmű kijelölése érdekében világosan meg kell különböztetni az adattárcák különböző összetevőit és konfigurációit. Adattárca-megoldás alatt az adattárca-szolgáltató által biztosított, az adattárca működtetéséhez szükséges teljes rendszer értendő. Ez magában foglal minden, az adattárca megfelelő működéséhez szükséges szoftver- és hardverkomponenst, valamint szolgáltatást, beállítást és konfigurációt. Az adattárca-megoldás telepíthető a felhasználók eszközeire és környezetébe is, illetve a szolgáltató háttérrendszeréből is szolgáltatható. Adattárcaegység alatt az adattárca-megoldás egyes felhasználókra szabott konkrét megvalósítása értendő. Ez magában foglalja az adattárca-felhasználó eszközére vagy környezetébe telepített, az adattárca-felhasználó által közvetlenül kezelt alkalmazást (a továbbiakban: adattárcapéldány), valamint a felhasználók adatainak és tranzakcióinak védelméhez szükséges biztonsági elemeket. E biztonsági elemeknek az érzékeny információk titkosítására és megőrzésére szolgáló speciális szoftvereket vagy hardvereket is tartalmazniuk kell. Az adattárcapéldánynak az adattárcaegység részét kell képeznie, és lehetővé kell tennie az adattárca-felhasználó számára, hogy hozzáférjen az adattárca funkcióihoz.

(6) Az adattárca-biztonsági kriptográfiai alkalmazások az adattárcaegységen belül különálló, egyedi összetevőkként nemcsak a kritikus eszközök, például a titkos kriptográfiai kulcsok védelméhez szükségesek, hanem egyes kulcsfontosságú funkciók biztosításához, például az elektronikus attribútumtanúsítványok megjelenítéséhez is. A közös technikai specifikációk alkalmazása megkönnyítheti a beágyazott biztonsági elemekhez való hozzáférést az adattárca-szolgáltatók számára. Az adattárca-biztonsági kriptográfiai alkalmazások különböző módokon és különböző típusú adattárca-biztonsági kriptográfiai eszközökhöz biztosíthatók. Amennyiben az adattárca-szolgáltató Java Card kisalkalmazások formájában biztosít egyedi adattárca-biztonsági kriptográfiai alkalmazásokat beágyazott biztonsági elemekhez, az adattárca-szolgáltatónak az I. mellékletben felsorolt szabványokat vagy az azokkal egyenértékű technikai specifikációkat kell követnie.

(7) Az adattárcaegységeknek lehetővé kell tenniük, hogy a személyazonosítóadat- vagy elektronikus attribútumtanúsítvány-szolgáltatók ellenőrizni tudják, hogy az említett adatokat vagy tanúsítványokat az adattárca-felhasználó valódi adattárcaegységeinek állítják ki.

(8) A beépített és alapértelmezett adatvédelem biztosítása érdekében az adattárcákat a legkorszerűbb adatvédelmi technikákkal kell ellátni. Ezeknek a funkcióknak lehetővé kell tenniük az adattárcák használatát anélkül, hogy felhasználójuk nyomon követhető lenne a különböző adattárca-igénybevevők között, amennyiben ez az adott használati mód esetén felmerülhetne. Az adattárca-szolgáltatóknak az adattárcaegység-tanúsítványok kapcsán fontolóra kell venniük a legkorszerűbb adatvédelmi kockázatcsökkentő intézkedések, például az önmegsemmisítő adattárca-tanúsítványok vagy a csoportos kibocsátás alkalmazását. Emellett a beágyazott közzétételi szabályzatnak figyelmeztetnie kell az adattárca-felhasználókat, hogy ügyeljenek az elektronikus attribútumtanúsítványokból származó attribútumok inadekvát vagy jogellenes nyilvánosságra hozatalára.

(9) Az adattárcaegység-tanúsítványnak lehetővé kell tennie az adattárcaegységtől attribútumokat lekérő adattárca-igénybevevők számára, hogy ellenőrizzék annak az adattárcaegységnek az érvényességi állapotát, amellyel kommunikálnak, mivel az adattárcaegység-tanúsítványokat vissza kell vonni, ha az adattárcaegység már nem minősül érvényesnek. Az adattárcaegységek érvényességi állapotára vonatkozó információkat interoperábilis módon kell rendelkezésre bocsátani, biztosítva, hogy azok minden adattárca-igénybevevő fél által felhasználhatók legyenek. Emellett azokban az esetekben, amikor az adattárca-felhasználók elveszítik adattárcaegységüket vagy az afölötti ellenőrzést, az adattárca-szolgáltatóknak lehetővé kell tenniük az adattárca-felhasználók számára, hogy kérjék adattárcaegységük visszavonását. A magánélet védelme és az összekapcsolhatóság kizárása érdekében a tagállamoknak az adattárcaegység-tanúsítványok esetében is alkalmazniuk kell a magánélet védelmét biztosító technikákat. Ezek magukban foglalhatják több, különböző rendeltetésű, csak az adott tranzakcióhoz szükséges minimális releváns adattárca-információit közzétevő adattárcaegység-tanúsítvány használatát, vagy a visszavonási azonosítók használatának alternatívájaként az adattárcaegység-tanúsítvány élettartamának korlátozását.

([8]) HL L 210., 2021.6.14., 51. o., ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 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).

(10) Annak garantálása érdekében, hogy valamennyi adattárca technikailag képes legyen határokon átnyúló helyzetekben a személyazonosító adatok és az elektronikus attribútumtanúsítványok fogadására és megjelenítésére anélkül, hogy az interoperabilitás sérülne, az adattárcáknak támogatniuk kell bizonyos előre meghatározott adatformátum-típusokat és a szelektív hozzáférhetővé tételt. A 910/2014/EU rendelet értelmében a szelektív hozzáférhetővé tétel azt a koncepciót jelöli, amely feljogosítja az adatok tulajdonosát arra, hogy egy nagyobb adatkészletnek csak bizonyos részeit tegye hozzáférhetővé annak érdekében, hogy az adatokat átvevő szervezet csak a felhasználó által kért szolgáltatás nyújtásához szükséges információkat szerezhesse meg. Mivel az adattárcáknak lehetővé kell tenniük, hogy a felhasználójuk szelektív módon tegye hozzáférhetővé az attribútumokat, a II. mellékletben felsorolt szabványokat oly módon kell alkalmazni, hogy ez a lehetőség rendelkezésre álljon az adattárcák esetében. Emellett az adattárcák más formátumokat és funkciókat is támogathatnak egyes konkrét felhasználási helyzetek megkönnyítése érdekében.

(11) A tranzakciók naplózása az átláthatóság biztosításának fontos eszköze, mivel áttekintést nyújt az ügyletekről az adattárca-felhasználónak. Emellett a naplózás arra is szolgálhat, hogy az adattárca-felhasználó kérésére lehetővé tegye bizonyos információknak az (EU) 2016/679 rendelet 51. cikke alapján létrehozott illetékes felügyeleti hatóságokkal való gyors és egyszerű megosztását az adattárca-igénybevevők gyanús magatartása esetén.

(12) Ahhoz, hogy az adattárca-felhasználó elektronikus aláírást használhasson, minősített elektronikus aláírást létrehozó eszközhöz kötött, minősített tanúsítványt kell kibocsátani a részére. Az adattárca-felhasználó számára hozzáférést kell biztosítani egy aláírás-létrehozó alkalmazáshoz. Míg a minősített tanúsítványok kibocsátása minősített bizalmi szolgáltatók által nyújtott szolgáltatás, a többi összetevőt az adattárca-szolgáltatók vagy más szervezetek biztosíthatják. Például a minősített elektronikus aláírást létrehozó eszközök kezeléséről minősített bizalmi szolgáltatók gondoskodhatnak szolgáltatás formájában, vagy azok lehetnek helyben telepítve az adattárca-felhasználó eszközére, például intelligens kártyaként. Hasonlóképpen, az aláírás-létrehozó alkalmazások is beépíthetők az adattárcapéldányba, lehetnek külön alkalmazások az adattárca-felhasználó eszközén, vagy távszolgáltatásként is működhetnek.

(13) Az adatexport- és adathordozhatósági objektumok naplózhatják a személyazonosító adatokat és az adott adattárcaegység számára kibocsátott elektronikus attribútumtanúsítványokat. Ezek az objektumok lehetővé teszik az adattárca-felhasználók számára, hogy – az adathordozhatósághoz való joguk megerősítése céljából – kinyerjék a releváns adatokat az adattárcaegységükből. A Bizottság arra ösztönzi az adattárca-szolgáltatókat, hogy azonos technikai megoldásokat alkalmazzanak az adattárcaegységek biztonsági mentési és adathelyreállítási folyamataihoz is, lehetővé téve az elveszett adattárcaegységek visszaszerzését vagy az adatoknak az egyik adattárca-szolgáltatótól a másikhoz történő továbbítását, amennyiben ez az adatvédelemhez való jog és a digitális személyazonossági ökoszisztéma biztonságának sérelme nélkül megvalósítható.

(14) Az adattárca-igénybevevőkre specifikus felhasználónevek generálása lehetővé teszi az adattárca-felhasználók számára, hogy anélkül hitelesítsék magukat, hogy szükségtelen adatokat kellene megadniuk az adattárca-igénybevevőknek. A 910/2014/EU rendelet rendelkezéseinek megfelelően az adattárca-felhasználókat semmi nem akadályozhatja abban, hogy álnéven férjenek hozzá a szolgáltatásokhoz, amennyiben a jogszabályok a hitelesítéshez nem írnak elő jogi személyazonosságot. Ezért az adattárcáknak rendelkezniük kell egy olyan funkcióval, amely generálni tud a felhasználó által választott és kezelt álneveket az online szolgáltatásokhoz való hozzáférés során történő hitelesítéshez. Az V. mellékletben meghatározott specifikációk alkalmazása során biztosítani kell e funkciók rendelkezésre állását. Az adattárca-igénybevevők ezen túlmenően nem kérhetik a felhasználóktól más adatok megadását, mint amelyek az igénybevevő nyilvántartásában az adattárcák tervezett felhasználására vonatkozóan meg vannak jelölve. Az adattárca-felhasználók számára lehetővé kell tenni, hogy bármikor ellenőrizhessék az igénybevevők nyilvántartási adatait.

(15) Az (EU) 2024/1183 rendelet értelmében a tagállamok nem korlátozhatják sem közvetlenül, sem közvetve azon természetes vagy jogi személyek köz- vagy magánszolgáltatásokhoz való hozzáférését, akik úgy döntenek, hogy nem használják az adattárcát, és kötelesek megfelelő alternatív megoldásokat elérhetővé tenni.

(16) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([10]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor az európai adatvédelmi biztossal, aki 2024. szeptember 30-án véleményt nyilvánított.

([10]) 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).

(17) Az e rendeletben előírt intézkedések összhangban vannak a 910/2014/EU rendelet 48. cikkében említett bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy és hatály

Ez a rendelet szabályokat állapít meg az adattárcák integritására és alapvető funkcióira vonatkozóan, amely szabályokat rendszeresen aktualizálni kell annak érdekében, hogy azok összhangban legyenek a technológia és a szabványok fejlődésével, valamint az (EU) 2021/946 ajánlás és különösen az architektúra és a referenciakeret alapján végzett munkával.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „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;

2. „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;

3. „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;

4. „személyazonosítóadat-szolgáltató”: az a természetes vagy jogi személy, aki vagy amely felelős a személyazonosító adatok kiállításáért és visszavonásáért, és garantálja azt, hogy a felhasználó személyazonosító adatai kriptográfiai eszközökkel egy adattárcaegységgel legyenek összekötve;

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

6. „adattárca-igénybevevő”: olyan igénybe vevő fél, amely digitális interakció útján köz- vagy magánszolgáltatások nyújtása céljából adattárcaegységeket szándékozik igénybe venni;

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

8. „adattárcaegység-tanúsítvány”: olyan adatobjektum, amely leírja az adattárca összetevőit, vagy lehetővé teszi ezen összetevők hitelességének ellenőrzését és érvényesítését;

9. „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;

10. „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;

11. „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;

12. „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;

13. „adattárca-kriptográfiai művelet”: az adattárca-felhasználó hitelességének ellenőrzéséhez, illetve a személyazonosító adatok vagy elektronikus attribútumtanúsítványok kibocsátásához vagy megjelenítéséhez szükséges kriptográfiai mechanizmus;

14. „adattárca-igénybevevői hozzáférési tanúsítvány”: az adattárca-igénybevevő hozzáférési tanúsítványának szolgáltatója által kibocsátott elektronikusbélyegző- vagy elektronikusaláírás-tanúsítvány, amely ellenőrzi és érvényesíti az adattárca-igénybevevő hitelességét;

15. „adattárca-igénybevevői hozzáférési tanúsítvány szolgáltatója”: az a természetes vagy jogi személy, akit vagy amelyet valamely tagállam megbíz azzal, hogy az adattárca-igénybevevői hozzáférési tanúsítványokat az adott tagállamban nyilvántartásba vett adattárca-igénybevevők számára kibocsássa.

II. FEJEZET

AZ EURÓPAI DIGITÁLIS SZEMÉLYIADAT-TÁRCÁK INTEGRITÁSA

3. cikk

Az adattárcaegység integritása

(1) Az adattárcaegységek mindaddig nem láthatják el a 910/2014/EU rendelet 5a. cikkének (4) bekezdésében felsorolt funkciókat, az adattárca-felhasználó adattárcaegységhez való hozzáférés céljából történő hitelesítésének kivételével, amíg az adattárcaegység sikeresen nem hitelesítette az adattárca-felhasználót.

(2) Az adattárca-szolgáltatók minden egyes adattárcaegységre vonatkozóan aláírással vagy bélyegzővel hitelesítenek legalább egy, a 6. cikkben meghatározott követelményeknek megfelelő adattárcaegység-tanúsítványt. Az adattárcaegység-tanúsítvány aláírásának vagy bélyegzővel ellátásának céljára használt tanúsítványt az (EU) 2024/2980 végrehajtási rendeletben említett, a megbízható szolgáltatók jegyzékében szereplő tanúsítvány alapján kell kibocsátani.

4. cikk

Adattárcapéldányok

(1) Az adattárcapéldányok a kritikus eszközök kezelésére legalább egy adattárca-biztonsági kriptográfiai eszközt használnak.

(2) Az adattárca-szolgáltatók garantálják az adattárcapéldányok és az adattárca-biztonsági kriptográfiai alkalmazások közötti kommunikáció integritását, hitelességét és titkosítását.

(3) Amennyiben a kritikus eszközök „magas” biztonsági szintű elektronikus azonosításhoz kötődnek, az adattárca kriptográfiai műveleteit vagy a kritikus eszközök adatait feldolgozó egyéb műveleteket a „magas” biztonsági szintű elektronikus azonosító eszközök jellemzőire és kialakítására vonatkozóan az (EU) 2015/1502 bizottsági végrehajtási rendeletben ([11]) meghatározott követelményeknek megfelelően kell végrehajtani.

5. cikk

Adattárca-biztonsági kriptográfiai alkalmazások

(1) Az adattárca-szolgáltatók garantálják, hogy az adattárca-biztonsági kriptográfiai alkalmazások:

a) csak akkor végeznek bármely, kritikus eszközöket érintő, az adattárca-felhasználó adattárcaegység általi hitelesítésétől eltérő egyéb adattárca-kriptográfiai műveleteket, ha a szóban forgó alkalmazások sikeresen hitelesítették az adattárca-felhasználót;

([11]) 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).

b) amennyiben „magas” biztonsági szintű elektronikus azonosítás kontextusában hitelesítik az adattárca-felhasználót, az adattárca-felhasználó hitelesítését a „magas” biztonsági szintű elektronikus azonosító eszközök jellemzőire és kialakítására vonatkozóan az (EU) 2015/1502 végrehajtási rendeletben meghatározott követelményeknek megfelelően végzik;

c) képesek új kriptográfiai kulcsok biztonságos létrehozására;

d) képesek a kritikus eszközök biztonságos törlésére;

e) képesek a titkos kulcsok birtoklási igazolását kiadni;

f) biztosítják az említett adattárca-biztonsági kriptográfiai alkalmazások által generált titkos kulcsok védelmét azok élettartama során;

g) megfelelnek a „magas” biztonsági szintű elektronikus azonosító eszközök jellemzőire és kialakítására vonatkozóan az (EU) 2015/1502 végrehajtási rendeletben meghatározott követelményeknek;

h) az összetevők közül egyedül képesek az adattárca kriptográfiai műveleteit és a kritikus eszközökkel végzett bármely más műveletet „magas” biztonsági szintű elektronikus azonosítással végrehajtani.

(2) Amennyiben az adattárca-szolgáltatók úgy döntenek, hogy egy beágyazott biztonsági elemhez adattárca-biztonsági kriptográfiai alkalmazást biztosítanak, műszaki megoldásukat az I. mellékletben felsorolt technikai specifikációkra vagy más egyenértékű műszaki előírásokra alapozzák.

6. cikk

Az adattárcaegység hitelessége és érvényessége

(1) Az adattárca-szolgáltatók biztosítják, hogy minden adattárcaegység tartalmazzon adattárcaegység-tanúsítványt.

(2) Az adattárca-szolgáltatók biztosítják, hogy az (1) bekezdésben említett adattárcaegység-tanúsítványok tartalmazzanak nyilvános kulcsokat, és hogy a megfelelő titkos kulcsokat adattárca-biztonsági kriptográfiai eszköz védje.

(3) Az adattárca-szolgáltatók:

a) tájékoztatják az adattárca-felhasználókat az adattárcaegységükkel kapcsolatos jogaikról és kötelezettségeikről;

b) kialakítják az adattárca-felhasználók biztonságos azonosítására és hitelesítésére szolgáló, az adattárcaegységektől független mechanizmusokat;

c) biztosítják, hogy az adattárca-felhasználók a (b) pontban említett hitelesítési mechanizmusok alkalmazásával kérelmezhessék adattárcaegység-tanúsítványaik visszavonását.

7. cikk

Az adattárcaegység-tanúsítványok visszavonása

(1) Az adattárca-szolgáltatók egyedüli entitásként jogosultak visszavonni az általuk létrehozott adattárcaegység-tanúsítványokat.

(2) Az adattárca-szolgáltatók nyilvánosan hozzáférhető szabályzatot dolgoznak ki, amelyben meghatározzák az adattárcaegység-tanúsítványok visszavonásának feltételeit és időkeretét.

(3) Amennyiben az adattárca-szolgáltatók visszavontak egyes adattárcaegység-tanúsítványokat, a visszavonást követő 24 órán belül tájékoztatják arról az érintett adattárca-felhasználókat, ideértve a visszavonás okát és az adattárca-felhasználót érintő következményeket is. Ezt a tájékoztatást tömören, könnyen hozzáférhető formában, világos és közérthető nyelven kell megfogalmazni.

(4) Amennyiben az adattárca-szolgáltatók visszavontak egyes adattárcaegység-tanúsítványokat, a magánélet védelmét tiszteletben tartva nyilvánosan is hozzáférhetővé teszik az adattárcaegység-tanúsítvány érvényességi státuszát, és megjelölik, hogy az adattárcaegység-tanúsítványban hol található meg ez az információ.

III. FEJEZET

AZ EURÓPAI DIGITÁLIS SZEMÉLYIADAT-TÁRCÁK ALAPVETŐ FUNKCIÓI ÉS JELLEMZŐI

8. cikk

A személyazonosító adatok és elektronikus attribútumtanúsítványok formátuma

Az adattárca-szolgáltatók biztosítják, hogy az adattárca-megoldások támogassák a II. mellékletben szereplő szabványjegyzéknek megfelelően kiállított személyazonosító adatok és elektronikus attribútumtanúsítványok használatát.

9. cikk

Tranzakciók naplózása

(1) Függetlenül attól, hogy a tranzakció sikeresen zárult-e, vagy sem, az adattárcapéldányoknak naplózniuk kell az adattárca-igénybevevőkkel és a más adattárcaegységekkel folytatott valamennyi tranzakciót, beleértve az elektronikus aláírást és bélyegzést is.

(2) A naplózott információknak legalább a következőket magukban kell foglalniuk:

a) a tranzakció időpontja és helye;

b) az adattárca-igénybevevő neve, elérhetőségi adatai és egyedi azonosítója, valamint a tagállam, ahol az említett adattárca-igénybevevő letelepedett, vagy más adattárcaegységek esetében az adattárcaegység-tanúsítványból származó releváns információk;

c) a tranzakció során lekért és megjelenített adatok típusa vagy típusai;

d) nem teljesített tranzakciók esetében a teljesítés elmaradásának oka.

(3) Az adattárca-szolgáltatók garantálják a naplózott információk integritását, hitelességét és titkosítását.

(4) Az adattárcapéldányok naplózzák az adattárca-felhasználó által az adattárcaegységen keresztül az adatvédelmi hatóságoknak küldött bejelentéseket.

(5) Az (1) és (2) bekezdésben említett naplóknak elérhetőknek kell lenniük az adattárca-szolgáltató számára, az adattárca-szolgáltatások nyújtásához szükséges mértékig és az adattárca-felhasználó kifejezett előzetes engedélyével.

(6) Az (1) és (2) bekezdésben említett naplóknak mindaddig hozzáférhetőknek kell maradniuk, amíg azt az uniós vagy a nemzeti jog megköveteli.

(7) Az adattárcaszolgáltatók lehetővé teszik az adattárca-felhasználók számára, hogy exportálni tudják a (2) bekezdésben említett naplózott információkat.

10. cikk

Beágyazott közzétételi szabályzatok

(1) Az adattárca-szolgáltatók biztosítják, hogy az általuk rendelkezésre bocsátott adattárcaegységek képesek legyenek kezelni a III. melléklet szerinti közös beágyazott közzétételi szabályzattal rendelkező elektronikus attribútumtanúsítványokat.

(2) Az adattárcapéldányoknak képeseknek kell lenniük együttesen kezelni és megjeleníteni az (1) bekezdésben említett beágyazott közzétételi szabályzatot és a megkereső adattárca-igénybevevőtől kapott adatokat.

(3) Az adattárcapéldányok ellenőrzik, hogy az adattárca-igénybevevő eleget tesz-e a beágyazott közzétételi szabályzat feltételeinek, és tájékoztatják az adattárca-felhasználót az ellenőrzés eredményéről.

11. cikk

Minősített elektronikus aláírások és bélyegzők

(1) Az adattárca-szolgáltatók gondoskodnak arról, hogy az adattárca-felhasználóknak rendelkezésére álljanak olyan minősített elektronikus aláírásokra vagy bélyegzőkre jogosító, minősített tanúsítványok, amelyek vagy az adattárca-példányra telepített, vagy külső eszközön található, vagy távolról szolgáltatott, minősített aláírást vagy bélyegzőt létrehozó eszközökhöz kapcsolódnak.

(2) Az adattárca-szolgáltatók biztosítják, hogy az adattárca-megoldások biztonságos kapcsolatot tudjanak létesíteni a minősített aláírást vagy bélyegzőt létrehozó alábbi eszközök valamelyik típusával: eszközre telepített, külső eszközön található vagy távolról szolgáltatott, minősített aláírást vagy bélyegzőt létrehozó eszközökkel, az (1) bekezdésben említett minősített tanúsítványok használata céljából.

(3) Az adattárca-szolgáltatók biztosítják, hogy a természetes személynek minősülő adattárca-felhasználók legalább nem szakmai célú használatra térítésmentes hozzáféréssel rendelkezzenek olyan aláírás-létrehozó alkalmazásokhoz, amelyek az (1) bekezdésben említett tanúsítványok felhasználásával lehetővé teszik minősített elektronikus aláírások díjmentes létrehozását.

12. cikk

Aláírás-létrehozó alkalmazások

(1) Az adattárcaegységek által használt aláírás-létrehozó alkalmazásokat adattárca-szolgáltatók, bizalmi szolgáltatók vagy adattárca-igénybevevők egyaránt biztosíthatják.

(2) Az aláírás-létrehozó alkalmazások a következő funkciókkal rendelkeznek:

a) az adattárca-felhasználó által szolgáltatott adatok aláírása vagy lebélyegzése;

b) az adattárca-igénybevevő által szolgáltatott adatok aláírása vagy lebélyegzése;

c) aláírások vagy bélyegzők létrehozása legalább a IV. mellékletben leírt kötelező formátumoknak megfelelően;

d) az adattárca-felhasználók tájékoztatása az aláírás- vagy bélyegző-létrehozási folyamat eredményéről.

(3) Az aláírás-létrehozó alkalmazások lehetnek az adattárcapéldányba beépített vagy külsők eszközök. Amennyiben az aláírás-létrehozó alkalmazások távoli minősített aláírás-létrehozó eszközökön alapulnak, illetve ha azok az adattárca-példányba beépítettek, támogatniuk kell a IV. mellékletben említett alkalmazásprogramozási felületet.

13. cikk

Adatexportálás és adathordozhatóság

Az adattárcaegységeknek – amennyiben ez technikailag megvalósítható és a kritikus eszközök kivételével – támogatniuk kell az adattárca-felhasználó személyes adatainak biztonságos exportálását és hordozhatóságát, garantálva, hogy az adattárca-felhasználó az (EU) 2015/1502 végrehajtási rendelet szerinti „magas” biztonsági szint mellett migráltathassa adatait egy másik adattárca-megoldás adattárcaegységére.

14. cikk

Álnevek

(1) Az adattárcaegységek az V. mellékletben meghatározott technikai specifikációknak megfelelően támogatják álnevek létrehozását az adattárca-felhasználók részére.

(2) Az adattárcaegységek támogatják az adattárca-igénybevevő kérésére az adott adattárca-igénybevevőre specifikus és egyedi álnevek generálását, és ezt az álnevet az adattárca-igénybevevő rendelkezésére bocsátják akár egymagában, akár az adott adattárca-igénybevevő által kért személyazonosító adatokkal vagy elektronikus attribútumtanúsítványokkal együtt.

IV. FEJEZET

ZÁRÓ RENDELKEZÉSEK

15. 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

AZ 5. CIKKBEN EMLÍTETT SZABVÁNYOK JEGYZÉKE

— SAM.01 Secured Applications for Mobile – Requirements for 3 third party Applets on eSIM and eSE through SAM [Harmadik felek által SAM használatával eSIM-re és eSE-re telepített kisalkalmazásokra vonatkozó előírások], v1.1 2023, GSMA;

— GPC_GUI_ 217 GlobalPlatform SAM Configuration – Technical specification for implementation of SAM [Technikai specifikáció a SAM alkalmazásához], v1.0 2024-04;

— GPC_SPE_0 34 GlobalPlatform Card Specification – Technical specification for smart cards [Technikai specifikáció intelligens kártyákhoz], v2.3.1 2018-03;

— GPC_SPE_0 07 GlobalPlatform Amendment A – Confidential Card Content Management [Bizalmas kártyatartalom-kezelés], v1.2 2019-07;

— GPC_SPE_0 13 GlobalPlatform Amendment D – Secure Channel Protocol 03 [Biztonságos csatorna protokoll 03], v1.2 2020-04;

— GPC_SPE_0 93 GlobalPlatform Amendment F – Secure Channel Protocol 11 [Biztonságos csatorna protokoll 11] v1.4 2024-03;

— GPD_SPE_ 0 75 Open Mobile API Specification (OMAPI API) for mobile apps to access secure elements on user devices [Open Mobile API specifikáció (OMAPI API) a felhasználói eszközön tárolt biztonságos elemek hozzáférését szolgáló mobilalkalmazásokhoz], v3.3 2018-08, GlobalPlatform.

II. MELLÉKLET

A 8. CIKKBEN EMLÍTETT SZABVÁNYOK JEGYZÉKE

— ISO/IEC.18013-5:2021

— „Verifiable Credentials Data Model 1.1.” [„Az ellenőrizhető hitelesítő tanúsítványok adatmodellje 1.1.”], W3C ajánlás, 2022. március 3.

III. MELLÉKLET

A 10. CIKKBEN EMLÍTETT KÖZÖS BEÁGYAZOTT KÖZZÉTÉTELI SZABÁLYZATOK JEGYZÉKE

1. „Nincs szabályzat”: az elektronikus attribútumtanúsítványokra nem vonatkozik szabályzat.
2. „Csak engedélyezett igénybevevők”: az adattárca-felhasználók az elektronikus attribútumtanúsítványokat csak a közzétételi szabályzatban kifejezetten felsorolt engedélyezett igénybevevőknek adhatják ki.
3. „Egyedi bizalomforrás”: az adattárca-felhasználók az elektronikus attribútumtanúsítványt csak olyan hitelesített adattárca-igénybevevőknek adhatják ki, amelyek adattárca-igénybevevői hozzáférési tanúsítványa egy adott gyökértanúsítványból (vagy a gyökértanúsítványok adott jegyzékében szereplő tanúsítványból), illetve köztes tanúsítvány(ok)ból származik.

IV. MELLÉKLET

A 12. CIKKBEN EMLÍTETT ALÁÍRÁSI ÉS BÉLYEGZŐFORMÁTUMOK

1. Kötelező aláírási vagy bélyegzőformátum:

   a) PAdES (PDF Advanced Electronic Signature), a következő szabvány szerint: ETSI EN 319 142-1 V1.1.1 (2016-04); Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures [Elektronikus aláírások és infrastruktúrák (ESI); PAdES digitális aláírások; 1. rész: Építőelemek és alapvető PAdES aláírások].

2. Opcionális aláírási vagy bélyegzőformátumok jegyzéke:

   a) XAdES, a következő szabvány szerint: ETSI EN 319 132-1 V1.2.1 (2022-02) – Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures (XAdES) [Elektronikus aláírások és infrastruktúrák (ESI); XAdES digitális aláírások; 1. rész: Építőelemek és alapvető XAdES aláírások], XML-formátumú aláírás esetén;

   b) JAdES, a következő szabvány szerint: ETSI TS 119 182-1 V1.2.1 (2024-07) – Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures [Elektronikus aláírások és infrastruktúrák (ESI); JAdES digitális aláírások; 1. rész: Építőelemek és alapvető JAdES aláírások], JSON-formátumú aláírás esetén;

   c) CAdES (CMS Advanced Electronic Signature), a következő szabvány szerint: ETSI EN 319 122-1 V1.3.1 (2023-06) – Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures [Elektronikus aláírások és infrastruktúrák (ESI); CAdES digitális aláírások; 1. rész: Építőelemek és alapvető CAdES aláírások], CMS-formátum aláírás esetén;

   d) ASiC (Associated Signature Container), a következő szabványok szerint: ETSI EN 319 162-1 V1.1.1 (2016-04) – Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers [Elektronikus aláírások és infrastruktúrák (ESI); Associated Signature Containers (ASiC); 1. rész: Építőelemek és alapvető ASiC tárolók] valamint ETSI EN 319 162-2 V1.1.1 (2016-04) – Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers [Elektronikus aláírások és infrastruktúrák (ESI); Associated Signature Containers (ASiC); 2. rész: További ASiC tárolók] a tárolók aláírásához.

3. Alkalmazásprogramozási felület:

   — Cloud Signature Consortium (CSC) specifikáció, v2.0 (2023. április 20.).

V. MELLÉKLET

A 14. CIKKBEN EMLÍTETT ÁLNÉVGENERÁLÁSRA VONATKOZÓ TECHNIKAI SPECIFIKÁCIÓK

Technikai specifikációk:

— WebAuthn – W3C ajánlás, 2021. április 8., 2-es szint, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.