2026/1731

2026.7.22.

A BIZOTTSÁG (EU) 2026/1731 VÉGREHAJTÁSI RENDELETE

(2026. július 15.)

az (EU) 2024/2977, az (EU) 2024/2979, az (EU) 2024/2980 és az (EU) 2024/2982 végrehajtási rendeletnek az alkalmazandó szabványok és specifikációk tekintetében történő módosításáról

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) Az európai digitális személyiadat-tárcák fejlesztése terén a tagállamok közötti lehető legmagasabb szintű harmonizáció biztosítása érdekében a tárcákra vonatkozó technikai specifikációk az (EU) 2021/946 bizottsági ajánlás ([2]) alapján végzett munkára – különösen az architektúrára és a referenciakeretre – támaszkodnak. Miután az architektúra és a referenciakeret jelentősen átalakult az (EU) 2024/2977 ([3]), az (EU) 2024/2979 ([4]), az (EU) 2024/2980 ([5]) és az (EU) 2024/2982 ([6]) bizottsági végrehajtási rendelet elfogadása óta, a felsorolt végrehajtási rendeleteket most módosítani kell azért, hogy összhangba kerüljenek az új szabványokkal, specifikációkkal és eljárásokkal.

A 910/2014/EU rendelet célkitűzéseivel összhangban a Bizottság kiválasztotta, mely szabványok vonatkoznak e konkrét követelmények teljesítésére. E szabványoknak tükrözniük kell a bevett gyakorlatokat, és széles körben elismertnek kell lenniük az érintett ágazatokban. Például, mivel – különösen az oktatási ágazatban – a W3C VCDM formátum használatos a tanúsítványok referenciaformátumaként, az európai digitális személyiadat-tárcáknak is támogatniuk kell ezt a formátumot, amint a W3C VCDM formátum új profiljai rendelkezésre állnak. Szükség esetén ezeket a szabványokat ki kell igazítani vagy ki kell egészíteni annak érdekében, hogy biztosítsák az európai digitális személyiadat-tárcák biztonságát és megbízhatóságát, ugyanakkor elősegítve a határokon átnyúló interoperabilitást és a belső piac hatékony működését.

(2) Az adattárca minden olyan használata esetén, amely az adattárca-felhasználó arcképének bemutatását igényli, az adattárca-megoldásoknak támogatniuk kell a szelektív hozzáférhetővé tétel funkcióját, és a hozzáférhetővé tételnek a felhasználó teljes körű ellenőrzése mellett kell történnie. A hozzáférhetővé tételről való döntési képesség és az arckép nem kívánt vagy felhatalmazás nélküli közzétételi kérelemmel szembeni védelme érdekében az európai digitális személyiadat-tárcák architektúrájának figyelmeztető mechanizmusokat kell biztosítania, és naplóznia kell az arckép használatával kapcsolatos minden tranzakciót. Annak biztosítása érdekében, hogy az adattárca-felhasználó tudjon a biometrikus adatok megosztásáról, a figyelmeztetéseknek jelezniük kell, hogy a kérelem biometrikus adatok

([1]) HL L 257., 2014.8.28., 73. o., ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) A Bizottság (EU) 2021/946 ajánlása (2021. június 3.) az európai digitális személyazonossági keretre irányuló összehangolt megközelítés közös uniós eszköztáráról (HL L 210., 2021.6.14., 51. o., ELI: http://data.europa.eu/eli/reco/2021/946/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).

([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 (HL L, 2024/2979, 2024.12.4., ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([5]) 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).

([6]) 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).

megosztásával jár, és kifejezetten elő kell írniuk, hogy a felhasználó megerősítse a hozzáférhetővé tételt. Amennyiben az igénybe vevő fél az arcképet egy természetes személy egyedi azonosítása vagy az adott személy állítólagos személyazonosságának igazolása céljából kezeli, az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([7]) 6. és 9. cikke, valamint az említett rendelet minden egyéb követelménye alkalmazandó, beleértve azt is, hogy az arckép igénybe vevő felek általi kezelésének a tervezett felhasználáshoz szükséges mértékre kell korlátozódnia. A tervezett felhasználásról az adatközlési kérelemmel együtt, világosan és közérthetően tájékoztatni kell az adattárca-felhasználót. A biometrikus adatok érzékenységének megfelelő figyelembevétele érdekében az adattárca-felhasználónak kifejezetten és konkrétan meg kell erősítenie, hogy hozzáférhetővé tehető az arckép. A hallgatólagos beleegyezés vagy az előre bejelölt jelölőnégyzetek nem tekinthetők az adattárca-felhasználó általi megerősítésnek. Az adattárca-felhasználó általi kifejezett megerősítésnek technikai biztosítéknak kell lennie, és önmagában nem adhat jogalapot az adatkezelésre. Az (EU) 2016/679 rendelet 9. cikkének (4) bekezdésében foglaltak szerint a tagállamok további feltételeket – köztük korlátozásokat – tarthatnak hatályban, illetve vezethetnek be a genetikai adatok, a biometrikus adatok és az egészségügyi adatok kezelésére vonatkozóan.

(3) Azért, hogy a tagállamok elegendő időt kapjanak nemzeti eljárásaik módosítására, az adattárca-felhasználó arcképe csak 2028. augusztus 11-től szerepelhet a természetes személy kötelező személyazonosító adatai között. Amennyiben az említett képek meglévő személyazonosító okmányokból, például személyazonosító igazolványokból vagy útlevelekből származnak, az (EU) 2025/1208 ([8]), illetve a 2252/2004/EK tanácsi rendeletekben ([9]) meghatározott vonatkozó követelmények alkalmazandók.

(4) A 910/2014/EU rendelet előírja, hogy az adattárcáknak képesnek kell lenniük az európai digitális személyiadat-tárca bizalmi jegyének megjelenítésére annak ellenőrizhető, egyszerű és felismerhető jelzéseként, hogy az adattárcát a rendelettel összhangban nyújtották. A bizalmi jegy használata támogatni fogja a belső piac hatékony működését, garantálja a tisztességes versenyt és védi a fogyasztók érdekeit. A bizalmi jegy használatának lehetővé tétele érdekében meg kell határozni a bizalmi jegy vizuális és műszaki jellemzőit.

(5) A 910/2014/EU rendelet 12b. cikkében foglaltak szerint a kapuőröknek lehetővé kell tenniük az európai digitális személyiadat-tárcák szolgáltatói és a bejelentett elektronikus azonosító eszközök kibocsátói számára az ugyanazon operációs rendszerrel, hardver- vagy szoftverfunkciókkal való tényleges interoperabilitást és azokhoz az interoperabilitás céljából való tényleges hozzáférést. Az ilyen tényleges interoperabilitást és hozzáférést díjmentesen kell biztosítani, függetlenül attól, hogy azon hardver- vagy szoftverfunkciók az operációs rendszer részét képezik-e, a kapuőr rendelkezésére állnak-e, vagy a kapuőr használja-e azokat az ilyen szolgáltatások nyújtása során. Mivel a használhatóság, a biztonság és a tagállamok közötti interoperabilitás biztosítása érdekében minden adattárca-megoldásnak támogatnia kell a protokollok és interfészek közös készletét, a kapuőröknek biztosítaniuk kell az e rendelet XII. mellékletében meghatározott protokollok és interfészek végrehajtásához szükséges operációs rendszert, hardver- vagy szoftverfunkciókat. Ebben az összefüggésben az eszközök közötti online adatátvitel során a kapuőröknek mind a fizikai közelség ellenőrzése, mind a két eszköz közötti adattovábbítás tekintetében előnyben kell részesíteniük a Client To Authenticator Protocol (CTAP) specifikáció 2.3. verziója ([10]) által biztosított helyi kommunikációs csatornát a CTAP hibrid alagút szolgáltatásainak használatával szemben.

(6) Azért, hogy a tagállamoknak, az adattárca-igénybevevői nyilvántartási tanúsítványok szolgáltatóinak és az adattárca-szolgáltatóknak elegendő idejük legyen arra, hogy lehetővé tegyék az adattárcaegységek számára az adattárca-igénybevevői nyilvántartási tanúsítványok hitelesítését és érvényesítését, ez a követelmény csak 2028. augusztus 11-től alkalmazandó.

(7) Az (EU) 2016/679 európai parlamenti és tanácsi rendelet és adott esetben a 2002/58/EK európai parlamenti és tanácsi irányelv ([11]) az e rendelet szerinti valamennyi személyesadat-kezelési tevékenységre alkalmazandó.

([7]) 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).

([8]) A Tanács (EU) 2025/1208 rendelete (2025. június 12.) az uniós polgárok személyazonosító igazolványai és a szabad mozgás jogával élő uniós polgárok és azok családtagjai részére kiállított tartózkodási okmányok biztonságának megerősítéséről (HL L, 2025/1208, 2025.6.20., ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) A Tanács 2252/2004/EK rendelete (2004. december 13.) a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról (HL L 385., 2004.12.29., 1. o., ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) A FIDO Alliance által javasolt szabvány, Client to Authenticator Protocol (CTAP), 2026. február 26.

([11]) 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).

(8) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([12]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2026. április 17-én véleményt ([13]) nyilvánított.

(9) Az e rendeletben előírt intézkedések összhangban vannak a 910/2014/EU rendelet 48. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

Az (EU) 2024/2977 végrehajtási rendelet módosításai

Az (EU) 2024/2977 végrehajtási rendelet a következőképpen módosul:

1. A szöveg a következő 3a. cikkel egészül ki:

„*3a. cikk*

Az arckép védelme

(1) Az (EU) 2016/679 rendelet szerinti tájékoztatási követelményeken túlmenően az adattárca-szolgáltatók biztosítják, hogy az általuk nyújtott adattárca-megoldások figyelmeztessék az adattárca-felhasználókat, amennyiben az adattárca-igénybevevők az arckép hozzáférhetővé tételét kérik, jelezve, hogy a kérelem biometrikus adatok megosztásával jár, és megerősítést igényel az arckép szelektív hozzáférhetővé tételéhez.

(2) Az arckép adattárca-igénybevevő részére történő szelektív hozzáférhetővé tételének végrehajtása érdekében az adattárca-szolgáltatók gondoskodnak arról, hogy az adattárca-megoldások előírják az adattárca-felhasználó számára, hogy kifejezetten és konkrétan erősítse meg, hogy az arckép megjeleníthető.

(3) Az adattárca-igénybevevők csak akkor őrizhetik meg az arcképet, ha annak kezelése az uniós adatvédelmi joggal összhangban történő azonosítás és hitelesítés céljából szükséges, vagy ha ezt az uniós vagy nemzeti jog az uniós adatvédelmi joggal összhangban előírja. Az arckép csak akkor továbbítható harmadik országoknak vagy nemzetközi szervezeteknek, ha azt az uniós adatvédelmi jog lehetővé teszi.”

2. A 4. cikk (1) bekezdésének helyébe a következő szöveg lép:

„(1) Az adattárcaegységek részére kibocsátott elektronikus attribútumtanúsítványoknak meg kell felelniük az (EU) 2024/2979 végrehajtási rendelet II. mellékletében meghatározott szabványok legalább egyikének.”

3. Az 5. cikkben a (4) bekezdés b) pontja helyébe a következő szöveg lép:

„b) azon adattárcaegység adattárcaegység-tanúsítványának visszavonása esetén, amelynek részére a személyazonosító adatokat kiállították;”

4. A melléklet helyébe e rendelet I. mellékletének szövege lép.

([12]) 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).

([13]) Az európai adatvédelmi biztos hivatalos észrevételei az alkalmazandó szabványokról és specifikációkról, valamint az (EU) 2024/2980 végrehajtási rendelet helyesbítéséről szóló végrehajtási rendelet tervezetéről | Az európai adatvédelmi biztos.

2. cikk

Az (EU) 2024/2979 végrehajtási rendelet módosításai

Az (EU) 2024/2979 végrehajtási rendelet a következőképpen módosul:

1. A 3. cikk (2) bekezdését el kell hagyni.

2. Az 5. cikk (1) bekezdésének a) pontja helyébe a következő szöveg lép:

„a) csak akkor végeznek adattárca-biztonsági kriptográfiai eszközben tárolt kritikus eszközöket érintő és az adattárca-felhasználó hitelesítéséhez nem szükséges adattárca-kriptográfiai műveleteket, ha a szóban forgó alkalmazások sikeresen hitelesítették az adattárca-felhasználót;”.

3. A rendelet szövege a következő 5a. cikkel egészül ki:

„*5a. cikk*

Kriptográfiai mechanizmusok

Az adattárca-szolgáltatók a 4. cikk (2) bekezdésének alkalmazásában kizárólag az Ia. mellékletben említett kriptográfiai mechanizmusokat használhatják.”

4. A 6. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) Az adattárca-szolgáltatók minden egyes adattárcaegységre vonatkozóan adattárcaegység-tanúsítványokat bocsátanak ki. Az adattárca-szolgáltatók oly módon látják el aláírással vagy bélyegzővel az adattárcaegység-tanúsítványokat, hogy az aláírások vagy bélyegzők az (EU) 2024/2980 végrehajtási rendelet II. melléklete 2. szakasza 1. pontjának h) alpontjával összhangban felsorolt tanúsítvánnyal hitelesíthetők legyenek.”;

b) a (2) bekezdés helyébe a következő szöveg lép:

„(2) Az adattárca-szolgáltatók biztosítják, hogy az (1) bekezdésben említett adattárcaegység-tanúsítványok megfeleljenek az Ib. mellékletben meghatározott technikai specifikációknak.”;

c) a (3) bekezdés b) pontjának helyébe a következő szöveg lép:

„b) olyan, biztonságos azonosítási és hitelesítési mechanizmusokat alakítanak ki az adattárca-felhasználók számára, amelyek függetlenek az adattárcaegységektől;”.

5. A 9. cikk (2) bekezdésének b) pontja helyébe a következő szöveg lép:

„b) a megfelelő adattárca-igénybevevő neve, elérhetőségi adatai és egyedi azonosítója, valamint a tagállam, ahol az említett adattárca-igénybevevő letelepedett;”.

6. A 10. cikk (1) bekezdésének helyébe a következő szöveg lép:

„(1) Az adattárca-szolgáltatók biztosítják, hogy az általuk rendelkezésre bocsátott adattárcaegységek képesek legyenek kezelni a III. melléklet szerinti közös beágyazott közzétételi szabályzatra alkalmazandó technikai specifikációknak megfelelően kibocsátott elektronikus attribútumtanúsítványokat.”

7. A 12. cikk a következőképpen módosul:

a) a (2) bekezdés c) pontja helyébe a következő szöveg lép:

„c) aláírások vagy bélyegzők létrehozása legalább a IV. mellékletben leírt kötelező aláírás- vagy bélyegzőformátumnak megfelelően;”

b) a (3) bekezdés helyébe a következő szöveg lép:

„(3) Az aláírás-létrehozó alkalmazások lehetnek az adattárcapéldányba beépített vagy külső eszközök.”;

c) a cikk a következő bekezdéssel egészül ki:

„(4) Az adattárcaegységek által használt aláírás-létrehozó alkalmazások legalább a IV. mellékletben említett alkalmazásprogramozási felületet támogatják.”

8. A 14. cikk (1) bekezdését el kell hagyni.

9. A rendelet szövege a következő 14a. cikkel egészül ki:

„*14a. cikk*

Az európai digitális személyiadat-tárca bizalmi jegye

(1) Az adattárca-szolgáltatók gondoskodnak arról, hogy az adattárcaegységeken szerepeljen az európai digitális személyiadat-tárca bizalmi jegye. Az európai digitális személyiadat-tárca bizalmi jegyének formátumát a VI. és a VII. melléklet határozza meg.

(2) Az adattárca-szolgáltatók gondoskodnak arról, hogy az adattárcaegységek biztosítsák az adattárca-felhasználók számára az adattárca-megoldás tanúsítási státuszának ellenőrzését lehetővé tevő információkhoz való hozzáférést. E célból az adattárca-szolgáltatók biztosítják, hogy az adattárca-megoldás nyilvántartásba vételét követően a megfelelő adattárcaegységek tartalmazzák az Európai Bizottság által az ellenőrzéshez rendelkezésre bocsátott URL-címeket. Az adattárca-szolgáltatók gondoskodnak arról, hogy az adattárcaegységeik hozzáférjenek az európai digitális személyiadat-tárcák bizalmi jegyeinek a VIII. mellékletben meghatározott technikai specifikációkkal összhangban lévő adataihoz.

(3) Az európai digitális személyiadat-tárca bizalmi jegyének referenciaszínei a Pantone 661 és 116; vagy kék (100 % cián + 67 % magenta + 0 % sárga + 40 % fekete) és sárga (0 % cián + 20 % magenta + 100 % sárga + 0 % fekete) négyszínnyomás használatakor; RGB színek használata esetén a referenciaszín kék (0 piros + 51 zöld + 153 kék) és sárga (255 piros + 204 zöld + 0 kék).

(4) Az európai digitális személyiadat-tárca bizalmi jegye csak akkor használható fekete-fehérben a VII. mellékletben meghatározottak szerint, ha a színek használata nem kivitelezhető.

(5) Amennyiben az európai digitális személyiadat-tárca bizalmi jegyét sötét háttéren használják, az negatív formátumban, azonos háttérszínnel is használható. Amennyiben az európai digitális személyiadat-tárca színes bizalmi jegye színes háttéren nehezen látható, az európai digitális személyiadat-tárca bizalmi jegye a háttérrel szembeni kontraszt erősítése érdekében vonallal határolható körbe.

(6) Az európai digitális személyiadat-tárca bizalmi jegyének legalább 64 × 85 pixel méretűnek kell lennie, 150 dpi felbontással.

(7) Az adattárca-szolgáltatók gondoskodnak az európai digitális személyiadat-tárca bizalmi jegyének olyan módon történő használatáról, amely lehetővé teszi annak az adattárcaegységnek az egyértelmű megjelölését, amelyhez az európai digitális személyiadat-tárca bizalmi jegye tartozik. Az európai digitális személyiadat-tárca bizalmi jegye társítható olyan grafikus vagy szöveges elemekkel, amelyek egyértelműen megjelölik azt az adattárcaegységet, amelyhez használják, feltéve, hogy ezek az elemek nem változtatják meg az európai digitális személyiadat-tárca bizalmi jegyeként való felismerhetőségét, és nem módosítják a tanúsított európai digitális személyiadat-tárcáknak a 910/2014/EU rendelet 5d. cikkében említett listájával való társítását.

(8) Adattárcaegység-tanúsítvány visszavonása esetén az adattárca-szolgáltatók gondoskodnak arról, hogy a szóban forgó adattárcaegységen a továbbiakban ne jelenjen meg az európai digitális személyiadat-tárca bizalmi jegye.”

10. A rendelet új Ia. és Ib. melléklettel egészül ki, amelyek szövegét e rendelet II. és III. melléklete tartalmazza.

11. A II. melléklet helyébe e rendelet IV. melléklete lép.

12. A III. melléklet helyébe e rendelet V. melléklete lép.

13. A IV. melléklet e rendelet VI. mellékletének megfelelően módosul.

14. Az V. mellékletet el kell hagyni.

15. Az e rendelet VII. mellékletében szereplő szöveg VI. mellékletként kerül beillesztésre.

16. Az e rendelet VIII. mellékletében szereplő szöveg VII. mellékletként kerül beillesztésre.

17. Az e rendelet IX. mellékletében szereplő szöveg VIII. mellékletként kerül beillesztésre.

3. cikk

Az (EU) 2024/2980 végrehajtási rendelet módosításai

Az (EU) 2024/2980 végrehajtási rendelet a következőképpen módosul:

1. Az 5. cikk (2) bekezdésének helyébe a következő szöveg lép:

„(2) Adott esetben a Bizottság jegyzéket állít össze, tart fenn és tesz közzé, amelyben szerepelnek az adattárca-szolgáltatókra, a személyazonosítóadat-szolgáltatókra, az adattárca-igénybevevői hozzáférési tanúsítványok szolgáltatóira és az adattárca-igénybevevői nyilvántartási tanúsítványok szolgáltatóira vonatkozóan a tagállamok által bejelentett, a II. melléklet 2., 3., 4. és 5. szakaszában említett információk.”

2. Az (EU) 2024/2980 végrehajtási rendelet II. melléklete az e rendelet X. mellékletében foglaltak szerint módosul.

4. cikk

Az (EU) 2024/2982 végrehajtási rendelet módosításai

Az (EU) 2024/2982 végrehajtási rendelet a következőképpen módosul:

1. Az 1. cikk 2. pontjának helyébe a következő szöveg lép:

„2. a személyazonosító adatok attribútumainak és az elektronikus attribútumtanúsítványoknak az adattárca-igénybevevők részére történő megjelenítése;”.

2. A 3. cikk a következőképpen módosul:

a) az 1. pont helyébe a következő szöveg lép:

„1. az adattárca-igénybevevőkkel folytatott interakciók során ellenőrizzék és érvényesítsék az adattárca-igénybevevői hozzáférési tanúsítványok hitelességét, anélkül hogy e folyamatok végrehajtását egy operációs rendszerre, böngészőprogramra vagy más közvetítő alkalmazásra ruháznák át;”

b) a 2. pontot el kell hagyni;

c) a 3. pont helyébe a következő szöveg lép:

„3. ellenőrizzék és érvényesítsék az adattárca-igénybevevői hozzáférési tanúsítványok felhasználásával benyújtott kérelmek hitelességét;”

d) a 4. pont helyébe a következő szöveg lép:

„4. ellenőrizzék és érvényesítsék az adattárca-igénybevevői nyilvántartási tanúsítvány hitelességét;”

e) az 5. pont helyébe a következő szöveg lép:

„5. az adattárca-felhasználók számára megjelenítsék az adattárca-igénybevevői hozzáférési tanúsítványokban szereplő információkat;”

f) a 8. pontot el kell hagyni;

g) a 9. pont helyébe a következő szöveg lép:

„9. ne jelenítsék meg a kért attribútumokat az adattárca-igénybevevőknek, amíg a következő lépéseket el nem végezték:

a) annak ellenőrzése, hogy az adattárcaegységbe beágyazott közzétételi szabályzatokat az (EU) 2024/2979 végrehajtási rendelet 10. cikkével összhangban dolgozták fel;

b) annak ellenőrzése, hogy az adattárca-felhasználók az adatok megjelenítését részben vagy egészben jóváhagyták;”.

3. A 4. cikk (1) bekezdésének helyébe a következő szöveg lép:

„(1) Az adattárca-szolgáltatók biztosítják, hogy az adattárca-megoldások támogassák a személyazonosító adatok és az elektronikus attribútumtanúsítványok adattárcaegységek részére történő kiállításához, illetve kibocsátásához az I. mellékletben meghatározott protokollokat és interfészeket.”

4. Az 5. cikk a következőképpen módosul:

   a) az (1) és a (2) bekezdés helyébe a következő szöveg lép:

   „(1) Az adattárca-szolgáltatók biztosítják, hogy az adattárca-megoldások a II. mellékletben meghatározott technikai specifikációknak megfelelően támogassák az attribútumok adattárca-igénybevevőknek történő megjelenítésére szolgáló protokollokat és interfészeket az online térben és – adott esetben – a fizikai térben történő használat során.

   (2) Az adattárca-szolgáltatók biztosítják, hogy a felhasználók kérésére az adattárcaegységek a II. mellékletben meghatározott technikai specifikációknak megfelelően válaszoljanak az adattárca-igénybevevők 3. cikkben említett, sikeresen hitelesített és érvényesített kérelmeire.”;

   b) az (5) bekezdést el kell hagyni.

5. A 8. cikk helyébe a következő szöveg lép:

„*8. cikk*

Hatálybalépés

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

A 3. cikk 4. pontja 2028. augusztus 11-től alkalmazandó.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.”

6. A mellékletet el kell hagyni.

7. Az e rendelet XI. mellékletében foglalt szöveg I. mellékletként kerül beillesztésre.

8. Az e rendelet XII. mellékletében foglalt szöveg II. mellékletként kerül beillesztésre.

5. 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, 2026. július 15-én.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

I. MELLÉKLET

„MELLÉKLET

A 3. cikk (3) bekezdésében említett, a személyazonosító adatokra vonatkozó technikai specifikációk

1. 1. pont: A természetes személyek azonosító adatai

1. táblázat

A természetes személyek szelektív hozzáférhetővé tételhez kötelezően megadandó személyazonosító adatai

Adatazonosító	Meghatározás
`family_name`	Annak a felhasználónak az aktuális vezetékneve(i) vagy családneve(i), akire a személyazonosító adatok vonatkoznak.
`given_name`	Annak a felhasználónak az aktuális utóneve(i), beleértve adott esetben a második utóneve(ke)t is, akire a személyazonosító adatok vonatkoznak.
`birth_date`	Nap, hónap és év, amikor az a felhasználó született, akire a személyazonosító adatok vonatkoznak.
`birth_place`	Az az ország – az ISO 3166-1 szabvány szerinti alpha-2 országkódjával azonosítva –, vagy pedig az az állam, tartomány, körzet vagy járás, ahol az a felhasználó született, akire a személyazonosító adatok vonatkoznak.
`nationality`	Egy vagy több, az ISO 3166-1 szabvány szerinti alpha-2 országkód, amely annak a felhasználónak az állampolgárságát adja meg, akire a személyazonosító adatok vonatkoznak.
`portrait`	Amennyiben a felhasználó – adott esetben – nem utasítja el kifejezetten, arról a felhasználóról készített arcképmás, akire a személyazonosító adatok vonatkoznak; az arcképmásnak meg kell felelnie az ISO/IEC 39794-5 szabványban, vagy a visszamenőleges kompatibilitás céljából az ISO/IEC 19794-5 szabvány 8.2., 8.3. és 8.4. szakaszában a szemből készített teljes képtípusra vonatkozóan meghatározott minőségi követelményeknek; az arcképmást kódolt képadatként kell megadni, az ISO/IEC 19794-5 szabvány 5. szakasza szerint fejlécek vagy tömbök nélkül, kivéve magukat a képadatokat (JPEG kép) – 2028. augusztus 11-től alkalmazandó.

— A tagállamok rendelkezhetnek úgy, hogy a felhasználónak lehetősége legyen megtagadni az arcképnek a személyazonosító adatok közé való felvételét

— A tagállamok biztosítják, hogy a szelektív hozzáférhetővé tétel minden egyes adatazonosítóra alkalmazandó legyen, beleértve az arcképet is

— Amennyiben a természetes személy születési ideje nem ismert, a tagállamok olyan megfelelő értékeket választanak, amelyek megfelelnek az e melléklet 4.1. vagy (adott esetben) 4.2. pontjában meghatározott specifikációknak

— Amennyiben a természetes személy állampolgársága ismeretlen, a tagállamok a „QU” értéket használják

— Amennyiben a természetes személy nem rendelkezik állampolgársággal, a tagállamok a „QS” értéket használják

— Amennyiben a felhasználó elutasítja az arcképnek az adatok közé való felvételét, a tagállamok üresen hagyják az értéket

2. táblázat

A természetes személyek fakultatívan megadható személyazonosító adatai, amelyekre a szelektív hozzáférhetővé tétel vonatkozik

Adatazonosító	Meghatározás
resident_address	Teljes cím, ahol a felhasználó, akire a személyazonosító adatok vonatkoznak, jelenleg tartózkodik, vagy ahol kapcsolatba lehet lépni vele (utcanév, házszám, város stb.).
resident_country	Annak az országnak az ISO 3166-1 szabvány szerinti alpha-2 országkódja, ahol azon felhasználó aktuális tartózkodási helye található, akire a személyazonosító adatok vonatkoznak.
resident_state	Állam, tartomány, körzet vagy járás, ahol azon felhasználó aktuális tartózkodási helye található, akire a személyazonosító adatok vonatkoznak.
resident_city	Település, város vagy falu, ahol azon felhasználó aktuális tartózkodási helye található, akire a személyazonosító adatok vonatkoznak.
resident_postal_code	A hely irányítószáma, ahol azon felhasználó aktuális tartózkodási helye található, akire a személyazonosító adatok vonatkoznak.
resident_street	A közterület neve, ahol azon felhasználó aktuális tartózkodási helye található, akire a személyazonosító adatok vonatkoznak, beleértve a házszámot és annak esetleges kiegészítését vagy utótagját is.
personal_administrative_-number	A személyazonosítóadat-szolgáltató által kiadott személyi nyilvántartási számok körében egyedi, ahhoz a felhasználóhoz rendelt érték, akire a személyazonosító adatok vonatkoznak. Amennyiben a tagállamok ezen attribútum feltüntetése mellett döntenek, a személyazonosító adatok kiállításának alapjául szolgáló elektronikus azonosítási rendszereikben meg kell határozniuk azokat az alapelveket, amelyeket ezekre az attribútumértékekre alkalmaznak, beleértve adott esetben az ezen érték feldolgozására vonatkozó konkrét feltételeket is.
family_name_birth	Annak a felhasználónak a születéskori vezetékneve(i) vagy családneve(i), akire a személyazonosító adatok vonatkoznak.
given_name_birth	Annak a felhasználónak a születéskori utóneve(i), beleértve adott esetben a második utóneve(ke)t is, akire a személyazonosító adatok vonatkoznak.
sex	Az alábbi értékek valamelyike: 0 = nem ismert; 1 = férfi; 2= nő; 3 = egyéb; 4 = interszex; 5 = diverz; 6 = nyitott; 9 = nem alkalmazandó. A 0, 1, 2 és 9 érték esetében az ISO/IEC 5218 alkalmazandó.
email_address	Annak a felhasználónak az e-mail-címe [az RFC 5322 szabványnak ([1]) megfelelően], akire a személyazonosító adatok vonatkoznak.

Adatazonosító	Meghatározás
`mobile_phone_number`	Annak a felhasználónak a mobiltelefonszáma, akire a személyazonosító adatok vonatkoznak (a számot a „+” jel előzi meg; ezt követi az országkód, majd maga a telefonszám).

([1]) P. Resnick, Ed., „Internet Message Format,” (Internetes üzenetformátum), RFC 5322, 2008. október.

2. 2. pont: A jogi személyek azonosító adatai

3. táblázat

A jogi személyek kötelezően megadandó személyazonosító adatai

Adatazonosító
Aktuális jogi elnevezés
A küldő tagállam által a technikai specifikációkkal összhangban, a határokon átnyúló azonosítás céljára létrehozott egyedi azonosító, amely időben a lehető legtartósabb.

— Amennyiben egy adatazonosító nem ismert az adott személy esetében, vagy a személyazonosító adatok keretében nem állítható ki más módon, a tagállamoknak az adott helyzetnek megfelelő attribútumértéket kell használniuk helyette

4. táblázat

A jogi személyek fakultatívan megadható személyazonosító adatai

Adatazonosító
Aktuális cím
Héaazonosító szám
Adónyilvántartási szám
Az (EU) 2017/1132 európai parlamenti és tanácsi irányelvben ([1]) említett európai egyedi azonosító
Az (EU) 2022/1860 bizottsági végrehajtási rendeletben ([2]) említett jogalany-azonosító (LEI)
Az 1352/2013/EU bizottsági végrehajtási rendeletben említett EORI-szám (gazdasági szereplők nyilvántartása és azonosítása) ([3])
A 389/2012/EU tanácsi rendelet 2. cikkének 12. pontja szerinti jövedéki szám ([4])

([1]) Az Európai Parlament és a Tanács (EU) 2017/1132 irányelve (2017. június 14.) a társasági jog egyes vonatkozásairól (kodifikált szöveg) (HL L 169., 2017.6.30., 46. o., ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) A Bizottság (EU) 2022/1860 végrehajtási rendelete (2022. június 10.) a 648/2012/EU európai parlamenti és tanácsi rendeletnek az adatszolgáltatás standardjai, formátumai, gyakorisága és módszerei, valamint szabályai tekintetében történő alkalmazására vonatkozó végrehajtás-technikai standardok megállapításáról (HL L 262., 2022.10.7., 68. o., ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) A Bizottság 1352/2013/EU végrehajtási rendelete (2013. december 4.) a szellemi tulajdonjogok vámhatósági érvényesítéséről szóló 608/2013/EU európai parlamenti és tanácsi rendeletben meghatározott formanyomtatványok kidolgozásáról (HL L 341., 2013.12.18., 10. o., ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) A Tanács 389/2012/EU rendelete (2012. május 2.) a jövedéki adók területén való közigazgatási együttműködésről és a 2073/2004/EK rendelet hatályon kívül helyezéséről (HL L 121., 2012.5.8., 1. o., ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. pont: A személyazonosító adatokra vonatkozó metaadatok

5. táblázat

A személyazonosító adatokra vonatkozó metaadatok

Adatazonosító	Meghatározás	Használat
`issuing_authority`	A személyazonosító adatokat kiállító közigazgatási hatóság neve vagy az adott tagállam ISO 3166 szabvány szerinti alpha-2 országkódja, amennyiben nincs a személyazonosító adatok kiállítására jogosult külön hatóság.	Kötelező
`issuing_country`	A személyazonosítóadat-szolgáltató székhelye szerinti ország vagy terület ISO 3166-1 szerinti alpha-2 országkódja.	Kötelező
`expiry_date`	A személyazonosító adatok igazgatási érvényességi időszaka lejártának napja (és lehetőség szerint pontos ideje).	Opcionális
`document_number`	A személyazonosítóadat-szolgáltató által a személyazonosító adatokhoz rendelt szám.	Opcionális
`issuing_jurisdiction`	A személyazonosító adatokat kiállító joghatóság országalegységének kódja az ISO 3166-2:2020 szabvány 8. pontjában meghatározottak szerint. A kód első felének meg kell egyeznie a kiállító ország kódjával.	Opcionális
`issuance_date`	A személyazonosító adatok igazgatási érvényességi időszaka kezdetének napja (és lehetőség szerint pontos ideje).	Opcionális

4. 4. pont: A természetes személyek azonosító adataihoz tartozó attribútumok kódolása

— A természetes személyek azonosító adatait az elektronikus attribútumtanúsítványokra alkalmazandó, az (EU) 2024/2979 végrehajtási rendelet II. mellékletének 5. (SD-JWT VC formátum) és 6. (ISO/IEC-mdoc formátum) szakaszában meghatározott szabványoknak megfelelően kell kiállítani. Az 5.2.2., 5.2.4., 5.2.5., EAA-6.1-03, 6.2.2., 6.2.3., 6.2.4. és 6.2.5. szakasz nem alkalmazandó

— A természetes személyek azonosító adatai kódolásának meg kell felelnie az e melléklet 4.1. és 4.2. pontjában foglalt technikai specifikációknak

4.1. A természetes személyek azonosító adatainak kódolása ISO/IEC-mdoc formátumban

— Az ISO/IEC-mdoc formátumú személyazonosító adatok tanúsítványtípusa: „eu.europa.ec.eudi.pid.1”. Az e mellékletben meghatározott személyazonosítóadat-attribútumok névterének azonosítója: „eu.europa.ec.eudi.pid.1”

— Amennyiben a személyazonosító adatok között olyan adatok találhatók, amelyek esetében nem határoztak meg adatazonosítókat ebben a mellékletben, ezeket az adatokat a belföldi személyazonosító adatokra vonatkozó olyan névtéren belül kell meghatározni, amelynek általános formátuma eu.europa.ec.eudi.pid.[ISO 3166-1 alpha-2 országkód vagy az ISO 3166-2 régiókód], amelyet opcionális pont- és verziószám követ

— Belföldi névtér használata esetén annak rendszerét – beleértve az összes adatazonosítót, azok meghatározását, használatát és kódolási formátumát – az (EU) 2025/1569 bizottsági végrehajtási rendelet ([1]) 8. cikkével összhangban közzé kell tenni

— Az e melléklet 1. és 3. pontjában meghatározott személyazonosító adatokat és metaadataikat az ISO/IEC mdoc formátum specifikációinak értelmében bele kell foglalni a személyazonosító adatelemekbe

— A MobileSecurityObject típusú példány deviceKeyInfo tagján belüli deviceKey tagnak tartalmaznia kell egy nyilvános kulcsot

— Az említett nyilvános kulcsnak meg kell egyeznie az adattárca-felhasználó adattárca-biztonsági kriptográfiai eszközében (a továbbiakban: WSCD eszköz) tárolt privát kulccsal

— A személyazonosító adatokat ISO/IEC-mdoc formátumban aláíró CB-AdES digitális aláírás védett fejlécének tartalmaznia kell az RFC 9360 ([2]) szabványban meghatározott x5u és x5t fejlécparamétert

— Az x5t fejlécparaméterben használt kivonatoló algoritmusnak az SHA-256 függvénynek kell lennie

— A személyazonosító adatok ISO/IEC-mdoc formátumban történő kódolására vonatkozó követelményeket a 6. táblázat tartalmazza

6. táblázat

A személyazonosító adatok ISO/IEC-mdoc formátumban történő kódolására vonatkozó követelmények

Adatazonosító	Attribútumazonosító	Kódolási formátum
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) A Bizottság (EU) 2025/1569 végrehajtási rendelete (2025. július 29.) a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített elektronikus attribútumtanúsítványok és a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok tekintetében történő alkalmazására vonatkozó szabályok megállapításáról (HL L, 2025/1569, 2025.7.30., ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) J. Schaad, „CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates" (https://datatracker.ietf.org/doc/rfc9360/).

Adatazonosító	Attribútumazonosító	Kódolási formátum
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate vagy full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate vagy full-date

— A 6. táblázatban meghatározott attribútumok kódolási formátumának jelölése az RFC 8610 ([3]) szabványban meghatározott megjelenítési típusokat használja, a következő kiegészítő követelményekkel:

a) a tstr formátumhoz UTF-8 kódolást kell alkalmazni;

b) a tstr formátumnak támogatnia kell a teljes Unicode tartományt;

c) a tstr hossza legfeljebb 150 karakter lehet;

d) a dátumot az RFC 8943 ([4]) szabványban meghatározottak szerint kell kódolni;

e) a teljes dátumot #6.1004(tstr) formában kell értelmezni, ahol az 1004 címke megfelel az RFC 8943 szabványban előírtaknak;

f) a tdate attribútumnak az RFC 3339 ([5]) szabványban meghatározott dátum-idő karakterláncot kell tartalmaznia;

g) a full-date attribútumnak az RFC 3339 szabványban meghatározott full-date karakterláncot kell tartalmaznia, az RFC 8943 szabványnak megfelelően;

h) eltérő rendelkezés hiányában a dátum attribútumokban való megjelenítésekor:

— nem használható a másodperc törtrésze

— nem használható az UTC-től számított helyi eltérés, és az RFC 3339 szabványban meghatározott időeltérésként „Z” értéket kell megadni

i) a 0 és 1 fő típusú egész számnak a lehető legkisebbnek kell lennie az RFC 8949 ([6]) szabvány 4.2. pontjában meghatározottak szerint;

j) a place_of_birth attribútumnak a következő kulcs-érték párok közül legalább egyet tartalmaznia kell: „country”, „region” vagy „locality”;

k) a bstr, tstr, tömb vagy térkép formátumban a hosszúságot a lehető legrövidebben kell kifejezni, az RFC 8949 szabvány 4.2. pontjában meghatározottak szerint;

([3]) C. Vigano és H. Birkholz, „Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures”, RFC 8610, 2019. június.
([4]) M. Jones, A. Nadalin és J. Richter, „Concise Binary Object Representation (CBOR) Tags for Date”, RFC 8943, 2020. november.
([5]) G. Klyne és C. Newman, „Date and Time on the Internet: Timestamps”, RFC 3339, 2002. július.
([6]) C. Bormann és P. Hoffman, „Concise Binary Object Representation (CBOR)”, RFC 8949, 2020. december.

l) az állampolgárság attribútumot az ISO 3166-1 szabványban meghatározott alpha-2 országkódok tömbjeként kell kódolni. Az RFC 8610 szabványban meghatározott CDDL jelölés használata esetén ezen attribútum kódolása a következő:

— nationalities = [+ CountryCode];

— CountryCode = tstr az ISO 3166-1 szabványban meghatározott alpha-2 országkód

— amennyiben az az adattárca-felhasználó, akire a személyazonosító adatok vonatkoznak, több állampolgársággal rendelkezik, és a személyazonosítóadat-szolgáltató igazolja ezen állampolgárságokat, a személyazonosítóadat-szolgáltató a személyazonosító adatokba belefoglalhatja az összes állampolgárságot

— a place_of_birth attribútumot place_of_birth típusúként kell kódolni. Az RFC 8610 szabványban meghatározott CDDL jelölés használata esetén ezen attribútum kódolása a következő:

place_of_birth =

{

? 'country' : tstr ; egyetlen, az ISO 3166-1 szabvány szerinti alpha-2 országkód

? 'region': tstr ; állam, tartomány, körzet vagy járás

? 'locality': tstr ; település, város vagy falu

}

4.2. A személyazonosító adatok SD-JWT VC formátumban történő kódolására vonatkozó követelmények

— Az e pontban meghatározott személyazonosító adatoknak és metaadataiknak az SD-JWT VC formátum specifikációinak értelmében állításokként kell szerepelniük a személyazonosító adatok között

— A kiállított személyazonosító adatokban szereplő, az előző franciabekezdésben említett valamennyi állításnak egyenként szelektíven felfedhetőnek kell lennie, kivéve azokat az állításokat, amelyeket az SD-JWT VC formátumban nem szelektíven felfedhetőként határoztak meg

— A 7. táblázat azoknak az állításneveknek a kódolását tartalmazza, amelyek nyilvános nevek

— A 8. táblázat a személyazonosító adatokra jellemző állításnevek kódolását tartalmazza

— Az SD-JWT VC formátumban kódolt személyazonosító adatokban használt JSON karakterlánchoz UTF-8 kódolást kell alkalmazni, és a karakterláncnak támogatnia kell a teljes Unicode tartományt, kivéve, ha az alábbi 8. táblázatban vagy az abban szereplő hivatkozásokban kifejezetten más van megadva

— Az RFC 7519 ([7]) szabványban meghatározott nbf és exp JWT-állításokat kell használni az SD-JWT VC formátumnak megfelelő személyazonosító adatok műszaki érvényességi idejének kifejezésére

([7]) J. Jones et al., „JSON Web Token (JWT)”, RFC 7519, 2015. május.

— A személyazonosító adatoknak tartalmazniuk kell az RFC 7800 ([8]) szabványban meghatározott cnf állítást, amely az adattárca-felhasználó adattárcaegységének WSCD eszközében tárolt privát kulcsból generált nyilvános kulcs

— Az SD-JWT VC formátumú személyazonosító adatok digitális aláírásának védett fejléce az RFC 7515 ([9]) szabványban meghatározott x5u és x5t#S256 fejlécparamétereket tartalmazza

7. táblázat

A személyazonosító adatok SD-JWT VC formátumban, nyilvános nevekkel történő kódolására vonatkozó követelmények

Adatazonosító	Attribútumazonosító	Kódolási formátum
`family_name`	`family_name`	karakterlánc
`given_name`	`given_name`	karakterlánc
`birth_date`	`birthdate`	karakterlánc, ISO 8601-1, ÉÉÉÉ-HH-NN formátum
`birth_place`	`place_of_birth`	JSON-struktúra
`nationality`	`nationalities`	karakterlánctömb
`resident_address`	`address.formatted`	karakterlánc
`resident_country`	`address.country`	karakterlánc
`resident_state`	`address.region`	karakterlánc
`resident_city`	`address.locality`	karakterlánc
`resident_postal_code`	`address.postal_code`	karakterlánc
`resident_street`	`address.street_address`	karakterlánc
`family_name_birth`	`birth_family_name`	karakterlánc
`given_name_birth`	`birth_given_name`	karakterlánc
`email_address`	`email`	karakterlánc
`mobile_phone_number`	`phone_number`	karakterlánc
`portrait`	`picture`	karakterlánc; base64 kódolású arcképet JPEG formátumban tartalmazó adat-URL

([8]) M. Jones et al., „Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)”, RFC 7800, 2016. április.
([9]) M. Jones et al., „JSON Web Signature (JWS)”, RFC 7515, 2015. május.

8. táblázat

A személyazonosító adatok SD-JWT VC formátumban, privát nevekkel történő kódolására vonatkozó követelmények

Adatazonosító	Attribútumazonosító	Kódolási formátum
`expiry_date`	`date_of_expiry`	karakterlánc, ISO 8601-1, ÉÉÉÉ-HH-NN formátum
`issuance_date`	`date_of_issuance`	karakterlánc, ISO 8601-1, ÉÉÉÉ-HH-NN formátum
`personal_administrative_number`	`personal_administrative_number`	karakterlánc
`sex`	`sex`	szám
`issuing_authority`	`issuing_authority`	karakterlánc
`issuing_country`	`issuing_country`	karakterlánc
`document_number`	`document_number`	karakterlánc
`issuing_jurisdiction`	`issuing_jurisdiction`	karakterlánc

— A személyazonosító adatok alaptípusának a vct állításban szereplő „urn:eudi:pid:1” karakterláncnak kell lennie. A típusokat minden személyazonosító adat esetében az „urn:eudi:pid:” névtérben kell használni

— Amennyiben a személyazonosító adatok olyan attribútumokat tartalmaznak, amelyeket e melléklet nem határoz meg, ezeket az attribútumokat egy belföldi típuson belül kell meghatározni

— Belföldi típus használata esetén annak rendszerét – beleértve az összes adatazonosítót, azok meghatározását, használatát és kódolási formátumát – az (EU) 2025/1569 végrehajtási rendelet 8. cikkével összhangban közzétett rendszerben kell meghatározni

5. 5. pont: A bizalmi infrastruktúrával kapcsolatos részletek

A személyazonosítóadat-szolgáltatók jegyzéke, amelyet az (EU) 2024/2980 végrehajtási rendelettel összhangban a Bizottság rendelkezésre bocsátott, lehetővé teszi a személyazonosító adatok hitelességének ellenőrzését.”

II. MELLÉKLET

„*Ia. MELLÉKLET*

Az 5a. cikkben említett kriptográfiai mechanizmusok

Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms" (Elfogadott kriptográfiai mechanizmusok), az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kiadványa ([1])."

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

III. MELLÉKLET

„Ib. MELLÉKLET

A 6. cikk (2a) bekezdésében említett, az adattárcaegység-tanúsítványokra vonatkozó technikai specifikációk

1. Az adattárcaegység-tanúsítvány egy vagy több adattárcapéldány-tanúsítványt és egy vagy több kulcstanúsítványt tartalmaz.

2. Az adattárcapéldány-tanúsítványnak és a kulcstanúsítványoknak meg kell felelniük a következő követelményeknek:

   a) A formátumra vonatkozó követelmények

      — FR-WIA-1: Az adattárcapéldány-tanúsítványnak az RFC 7519 ([1]) szabványban meghatározott JSON Web Token (JWT) formátumúnak kell lennie, amelyet az adattárca-szolgáltatónak kompakt alapvető B JAdES aláírással vagy bélyegzővel kell ellátnia

         — FR-WIA-1.1: Az adattárcapéldány-tanúsítványnak az OpenID for Verifiable Credential Issuance 1.0 verziójának ([2]) (OID4VCI) E. függelékében meghatározott és az alábbi C-WIA-1 és C-WIA-2 pont szerint kibővített adattárca-tanúsítványnak kell lennie

      — FR-KA-1: A kulcstanúsítványnak az RFC 7519 szabványban meghatározott JWT formátumúnak kell lennie, amelyet az adattárca-szolgáltatónak kompakt alapvető B JAdES aláírással vagy bélyegzővel kell ellátnia

         — FR_KA_1.1: A kulcstanúsítványnak az OID4VCI szabvány D. függelékében meghatározott és az alábbi C_KA-1 és C_KA-2 pont szerint kibővített kulcstanúsítványnak kell lennie

   b) Átvitelre vonatkozó követelmények

      — TR-WIA-1: Az adattárcaegységnek adattárcapéldány-tanúsítványt kell alkalmaznia a személyazonosító adatok, minősített vagy nem minősített elektronikus attribútumtanúsítványok vagy a hiteles forrásért felelős közigazgatási szerv által vagy nevében rendelkezésre bocsátott elektronikus attribútumtanúsítványok kiállítása, illetve kibocsátása során

      — TR-WIA-2: Az adattárca-szolgáltatónak ellenőriznie kell az adattárcapéldány integritását, és aláírással vagy bélyegzővel kell ellátnia az adattárcapéldány-tanúsítványt

         — TR-WIA-2.1: Amennyiben az adattárca-szolgáltató adattárcapéldány-tanúsítványt bocsát ki, az adattárca-szolgáltató által az adattárcapéldány integritása tekintetében végzett ellenőrzés időpontja és a kibocsátott adattárcapéldány-tanúsítvány „exp” fejlécparaméterében feltüntetett időpont közötti különbségnek 24 óránál rövidebbnek kell lennie

         — TR-WIA-2.2: Az adattárca-szolgáltatónak biztosítania kell, hogy az adattárcaegység tartalmazzon a személyazonosító adatok és az elektronikus attribútumtanúsítványok kiállításához, illetve kibocsátásához szükséges adattárcapéldány-tanúsítványokat

      — TR-WIA-3: A kibocsátás során az adattárcaegységnek az OID4VCI szabványban meghatározottak szerint adattárcapéldány-tanúsítványt kell küldenie az engedélyezési szervernek a leküldött engedélykérelemben és a tokenkérelemben

         — TR-WIA-3.1: Az adattárcaegységnek az OID4VCI szabvány E. függelékében meghatározott birtoklási igazolással (Proof-of-Possession, PoP) együtt kell elküldenie az adattárcapéldány-tanúsítványt

         — TR-WIA-3.2: Az adattárcaegység csak egy engedélyezési szervernek küldheti el ugyanazt az adattárcapéldány-tanúsítványt

([1]) RFC 7519: JSON Web Token (JWT), 2015. május.
([2]) OpenID for Verifiable Credential Issuance 1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: Amennyiben az adattárca-szolgáltató az alábbi R_WIA_1 pontban meghatározott „per-issuer reuse” opciót alkalmazza, az adattárcaegység többször is elküldheti az adattárcapéldány-tanúsítványt ugyanannak az engedélyezési szervernek

— TR-WIA-3.2.2: Amennyiben az adattárca-szolgáltató nem alkalmazza a „per-issuer reuse” opciót, az adattárcaegység legfeljebb egy kibocsátási folyamat során használhatja az adattárcapéldány-tanúsítványt

— TR-WIA-4: Amennyiben egy engedélyezési szerver adattárcapéldány-tanúsítványt kap, ellenőriznie kell az adattárcapéldány-tanúsítvány aláírását az adattárcapéldány-tanúsítvány JOSE fejlécében szereplő „x5c” paraméterben megadott aláírási tanúsítvány nyilvános kulcsával

— TR-WIA-4.1: Az engedélyezési szervernek azt is ellenőriznie kell, hogy a szóban forgó aláírási tanúsítvány ellenőrizhető-e az adattárca-szolgáltatóknak az (EU) 2024/2980 végrehajtási rendelet 5. cikkében említett jegyzékében szereplő bizalmi horgony segítségével, potenciálisan az x5c paraméterben megadott köztes tanúsítványok felhasználásával

— TR-WIA-4.2: Az engedélyezési szervernek ellenőriznie kell, hogy nem járt-e le az adattárcapéldány-tanúsítvány

— TR-WIA-4.3: Az engedélyezési szervernek ellenőriznie kell a PoP igazolás aláírását a „cnf” állításban szereplő nyilvános kulccsal

— TR_KA-1: Az adattárcaegységnek kulcstanúsítványt kell alkalmaznia a személyazonosító adatok kiállítása során, illetve az eszközhöz kötött, minősített vagy nem minősített elektronikus attribútumtanúsítványok vagy a hiteles forrásért felelős közigazgatási szerv által vagy nevében rendelkezésre bocsátott elektronikus attribútumtanúsítványok kibocsátása során

— TR_KA-1.1: Az adattárcaegység nem alkalmazhat kulcstanúsítványt az eszközhöz nem kötött, minősített vagy nem minősített elektronikus attribútumtanúsítványok vagy a hiteles forrásért felelős közigazgatási szerv által vagy nevében rendelkezésre bocsátott elektronikus attribútumtanúsítványok kibocsátása során

— TR_KA-2: Az adattárca-szolgáltatónak az adattárcaegység WSCD eszközéhez és annak minden egyes kulcstárolójához különböző kulcstanúsítványokat kell az adattárcaegység rendelkezésére bocsátania

— TR_KA-2.1: Az adattárca-szolgáltatónak aláírással vagy bélyegzővel kell ellátnia a kulcstanúsítványt, miután ellenőrizte, hogy a kulcstanúsítványban igazolt kulcsokat a kulcstanúsítványban ismertetett adattárcaegység vagy kulcstár WSCD eszközében tárolják

— TR_KA-2.2: A kulcstanúsítványnak legalább egy igazolt nyilvános kulcsot kell tartalmaznia. A hitelesítőadat-kibocsátónak küldött kulcstanúsítványban szereplő kulcsok száma nem haladhatja meg az adott hitelesítőadat-kibocsátó által a hitelesítőadat-kibocsátói metaadatokban meghatározott maximális kötegméretet; lásd: ETSI TS 119 472-3 ([3]), „credential_configurations_supported.credential_metadata.credential_reuse_policy.options.batch_size” paraméter

— TR_KA-2.3: Az adattárca-szolgáltatónak (az adattárcaegység WSCD eszközében vagy kulcstárában tárolt titkos kulcsnak megfelelő) nyilvános kulcsot kell elhelyeznie legfeljebb egy kulcstanúsítványban

— TR_KA-2.4: Az adattárcaegység egy kulcstanúsítványt legfeljebb egy hitelesítőadat-kibocsátási vagy -újrakibocsátási folyamat során használhat

— TR_KA-2.5: Az adattárca-szolgáltatónak biztosítania kell, hogy az adattárcaegység rendelkezzen a személyazonosító adatok és az eszközhöz kötött elektronikus attribútumtanúsítványok kiállításához, illetve kibocsátásához szükséges kulcstanúsítványokkal

([3]) ETSI, „Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles” (Elektronikus aláírások és infrastruktúrák [ESI]; JAdES digitális aláírások; 3. rész: JAdES-szintek és alapprofilok), ETSI TS 119 472-3, V1.1.1, 2026. március.

— TR_KA-3: Amennyiben a kibocsátás során szükséges, az adattárcaegységnek az OID4VCI szabványban meghatározottak szerint a hitelesítőadat-kibocsátóhoz intézett hitelesítőadat-kérés „proofs” mezőjében „jwt” vagy „attestation” típusú igazolás formájában kulcstanúsítványt kell tartalmaznia

— TR_KA_3.1: Amennyiben az adattárcaegység „jwt” elem formájában tartalmaz kulcstanúsítványt, a kulcstanúsítványt a „key_attestation” objektumon belül az „attested_keys” tömb 0. indexében szereplő nyilvános kulcshoz tartozó privát kulccsal kell aláírnia vagy lebélyegeznie

— TR_KA-4: Amennyiben a hitelesítőadat-kibocsátó eszközhöz kötött hitelesítő adatokat bocsát ki, a kibocsátói hitelesítő metaadatok között a „proof_types_supported” paraméterben az OID4VCI 12.2.4. szakaszában meghatározottak szerint fel kell tüntetnie, hogy mind a „jwt”, mind az „attestation” igazolástípust támogatja azon kulcstanúsítványok esetében, amelyeknek tartalmazniuk kell a „key_attestations_required” objektumot

— TR_KA-4.1: Amennyiben egy hitelesítőadat-kibocsátó eszközhöz nem kötött hitelesítő adatokat bocsát ki, a hitelesítőadat-kibocsátó metaadataiból ki kell hagynia a „proof_types_supported” és a „cryptographic_binding_methods_supported” paramétereket

— TR_KA-5: Amennyiben egy hitelesítőadat-kibocsátó „jwt” vagy „attestation” igazolástípusú kulcstanúsítványt kap, ellenőriznie kell a kulcstanúsítvány aláírását a kulcstanúsítvány JOSE fejlécében szereplő „x5c” paraméterben megadott aláírási tanúsítvány nyilvános kulcsával, valamint azt, hogy ez az aláírási tanúsítvány ellenőrizhető-e az adattárca-szolgáltatóknak az (EU) 2024/2980 végrehajtási rendelet 5. cikkében említett jegyzékében szereplő bizalmi horgony segítségével, potenciálisan az „x5c” paraméterben megadott köztes tanúsítványok felhasználásával

— TR_KA-6: Amennyiben egy hitelesítőadat-kibocsátó „jwt” igazolástípusú kulcstanúsítványt kap, ellenőriznie kell a „jwt” elem aláírását a „jwt” elemben szereplő „key_attestation” objektumon belül az „attested_keys” tömb 0. indexében szereplő kulccsal

— TR_KA-6.1: A hitelesítőadat-kibocsátónak ellenőriznie kell, hogy a „jwt” elem „nonce” mezője tartalmaz-e a nonce_endpointtól származó érvényes c_nonce értéket, az OID4VCI szabványban meghatározottak szerint

— TR_KA-7: Amennyiben a hitelesítőadat-kibocsátó „attestation” igazolástípusú kulcstanúsítványt kap, ellenőriznie kell, hogy a „key_attestation” objektum tartalmaz-e a nonce_endpointtól származó érvényes c_nonce értéket

— TR_KA-8: A személyazonosítóadat-szolgáltatónak biztosítania kell, hogy a személyazonosító adatok egy WSCD eszközt említő kulcstanúsítványból származó nyilvános kulcshoz legyenek kötve

c) A tartalomra vonatkozó követelmények

— C_WIA-1: Az adattárcapéldány-tanúsítványnak a következőket kell tartalmaznia:

— az OID4VCI szabvány E. függelékében meghatározott „wallet_name” állítás, amelynek értéke az adattárca-szolgáltatóknak az (EU) 2024/2980 végrehajtási rendelet 5. cikkében említett jegyzékében található adattárca-megoldás azonosítója

— „wallet_version” állítás ([4]), amely egy olyan karakterlánc, amelynek értéke az adattárca-megoldás verziója

— „wallet_solution_certification_information” állítás, amely olyan JSON-objektum, amely információkat tartalmaz az adattárca-megoldást tanúsító megfelelőségértékelő szervezetről, adott esetben a tanúsítási számról, valamint a tanúsítással kapcsolatos egyéb releváns részletekről

([4]) Ez az állítás ebben a bizottsági végrehajtási rendeletben kerül meghatározásra, mivel nem része az OID4VCI specifikációnak.

— „client_status” állítás, amely két almezőt tartalmaz:

— „status”: az OID4VCI szabvány E. függelékében meghatározott állapotlista-hivatkozás, amely az adattárcapéldány visszavonási állapotát jelzi. A részleteket lásd az alábbi e) szakaszban

— „exp”: az RFC 7519 szabványban meghatározott NumericDate érték, amely meghatározza azt az időpontot, ameddig az adattárca-szolgáltató megőrzi a visszavonási állapotot a „status” mezőben szereplő állapotlista-indexben

— az OID4VCI szabvány E. függelékében meghatározott „exp” állítás

— *MEGJEGYZÉS*: Az adattárcapéldány-tanúsítványban szereplő „client_status.status” állítás az adattárcapéldány visszavonási állapotát jelenti, nem pedig magának a tanúsítványnak a visszavonási állapotát. Ahogy az alábbi R_WIA-1 pontban szerepel, az adattárca-szolgáltató dönthet úgy, hogy minden egyes adattárcapéldány-tanúsítványt egy adott engedélyezési szerverhez rendel annak alapján, hogy az adott szerverre küldött valamennyi tanúsítvány ugyanazt az indexértéket tartalmazza a „client_status.status” bejegyzésben

— *MEGJEGYZÉS*: A „status” állításban szereplő „idx” érték az adattárcapéldány és az adattárcaegység (páros) egyedi azonosítójaként használható

— C_WIA-2: Az adattárcapéldány-tanúsítványnak az OID4VCI szabvány E. függelékében meghatározott „wallet_link” állítást is tartalmaznia kell, és ezen állításnak olyan URI értékkel kell rendelkeznie, amelyből további információk szerezhetők az adattárca-megoldásról

— C_WIA-3: Az engedélyezési szerver nem értelmezheti az adattárcapéldány-tanúsítvány felső szintjén szereplő „exp” paramétert az adattárcapéldány visszavonási állapotára vonatkozó megőrzési időtartam végeként

— *MEGJEGYZÉS*: Az adattárcapéldány-tanúsítvány felső szintjén szereplő „exp” paraméter azt jelzi, hogy mikor jár le maga a tanúsítvány

— C_KA-1: A kulcstanúsítványnak legalább a következőket kell tartalmaznia:

— az OID4VCI szabvány D. függelékében meghatározott „key_storage” és „user_authentication” állítások

— A „key_storage” és a „user_authentication” attribútumok értéke „iso_18045_high” kell, hogy legyen, amennyiben a kulcstanúsítvány WSCD eszközről tesz említést

— az OID4VCI szabvány D. függelékében meghatározott „certification” állítás, amely olyan URL-címet tartalmaz, amelyen információk szerezhetők be a WSCD eszköz vagy kulcstár által elért tanúsításról, indikatív jelleggel a rendszerről – például Common Criteria vagy GlobalPlatform –, az értékelt követelményekről – például az alkalmazandó védelmi profilról –, valamint az értékelési szintről

— Ezen információk alapján megállapíthatónak kell lennie, hogy a kulcstároló WSCD eszköz-e

— a „key_storage_status” állítás, amely két almezőt tartalmaz:

— „status”: az OID4VCI szabvány D.1. függelékében meghatározott állapotlista-hivatkozás. Az érték vagy a WSCD eszköz, vagy a tanúsított kulcsok tárolására használt kulcstártípus visszavonási állapotát, vagy – a per-key-attestation indexlehetőség keretében – egy egyedi adattárcaegység WSCD eszközének vagy kulcstárának visszavonási állapotát jelöli. A rendelkezésre álló index-hozzárendelési lehetőségeket lásd az alábbi R_KA_1 pontban

— „exp”: az RFC 7519 szabványban meghatározott NumericDate érték, amely meghatározza azt az időpontot, ameddig az adattárca-szolgáltató megőrzi a visszavonási állapotot a „status” mezőben szereplő állapotlista-indexben

— az OID4VCI szabvány D. függelékében meghatározott „exp” állítás

— *MEGJEGYZÉS* a kulcstanúsítványban szereplő „key_storage_status.status” állítás „idx” értékéhez: Amennyiben az adattárca-szolgáltató a „type-shared index” lehetőséget használja (lásd alább az R_KA_1 pontot), az azonos típusú WSCD eszközre vagy kulcstárra vonatkozó valamennyi kulcstanúsítványnak ugyanaz az állapotlista-indexe. Ezért az „idx” érték adattárcaegységenként nem egyedi. Ezzel szemben, ha az adattárca-szolgáltató a „per-key-attestation” lehetőséget használja, az „idx” az adattárcaegységre jellemző egyedi érték (vagy hitelesítőadat-kibocsátónként párosával egyedi). A hitelesítőadat-kibocsátó azonban egyetlen esetben sem használhatja a kulcstanúsítványban szereplő „idx” értéket adattárcaegység-azonosítóként, hanem az adattárcapéldány-tanúsítványban szereplő „idx” értéket kell használnia

— C_KA-2: Ha a kulcstanúsítványt „attestation” igazolástípusúként küldik el, annak tartalmaznia kell az OID4VCI szabvány F.3. függelékében meghatározott érvényes c_nonce értéket is

— C_KA-3: A hitelesítőadat-kibocsátó nem értelmezheti a kulcstanúsítvány felső szintjén szereplő „exp” paramétert a WSCD eszköz vagy kulcstár visszavonási állapotára vonatkozó megőrzési időtartam végeként

— *MEGJEGYZÉS*: A kulcstanúsítvány felső szintjén szereplő „exp” paraméter azt jelzi, hogy mikor jár le maga a kulcstanúsítvány

d) Az életciklusra vonatkozó követelmények

— Ez a melléklet a következő hitelesítőadat-kibocsátói metaadat-paramétereket határozza meg:

— „preferred_client_status_period”: OPTIONAL. Az adattárcaegység által a kibocsátás során megjelenítendő adattárcapéldány-tanúsítvány preferált fennmaradó állapotmegőrzési időtartamát másodpercben meghatározó egész szám. A fennmaradó állapotmegőrzési időtartamát a tanúsítványban szereplő „client_status.exp” értékének és a tanúsítvány kézhezvételi időpontjának a különbsége

— „preferred_key_storage_status_period”: OPTIONAL. Az adattárcaegység által a kibocsátás során megjelenítendő kulcstanúsítvány preferált fennmaradó állapotmegőrzési időtartamát másodpercben meghatározó egész szám. A fennmaradó állapotmegőrzési időtartam a tanúsítványban szereplő „key_storage_status.exp” értéknek és a tanúsítvány kézhezvételi időpontjának a különbsége

— LC_WIA-1: Az engedélyezési szerver az adattárcapéldány-tanúsítványokban úgy jelezheti a fennmaradó állapotmegőrzési időtartamra vonatkozó preferenciáit, hogy megadja a „preferred_client_status_period” metaadat-paramétert a hitelesítőadat-kibocsátó metaadat-végpontjában, az OID4VCI szabvány 12.2.2. szakaszában meghatározottak szerint

— LC_WIA-1.1: Ezt a mezőt a hitelesítőadat-kibocsátó metaadatainak felső szintjén kell elhelyezni

— LC_WIA_2: Az engedélyezési szerver nem értelmezheti az adattárcapéldány-tanúsítvány felső szintjén szereplő „exp” paramétert az adattárcapéldány visszavonási állapotára vonatkozó megőrzési időtartam végeként

— LC_WIA_3: Amennyiben az adattárca-szolgáltató aláírással vagy bélyegzővel lát el egy adattárcapéldány-tanúsítványt, az adott adattárcapéldány visszavonási állapotát mindaddig meg kell őriznie, amíg az adott adattárcapéldány-tanúsítványban feltüntetett „wallet_instance_status.exp” idő el nem telik

— LC_KA-1: Amennyiben kulcstanúsítvány szükséges, a hitelesítőadat-kibocsátó a kulcstanúsítványokban úgy jelezheti a fennmaradó állapotmegőrzési időtartamra vonatkozó preferenciáit, hogy megadja a fent leírt „preferred_key_storage_status_period” metaadat-paramétert a hitelesítőadat-kibocsátó metaadat-végpontjában, az OID4VCI 12.2.2. szakaszában meghatározottak szerint

— LC_KA-1.1: Ezt a mezőt a „key_attestations_required” objektumon belül kell elhelyezni, az OID4VCI 12.2.4. szakaszában meghatározottak szerint

— LC_KA-2: Az adattárca-szolgáltató választja meg az általa kibocsátott kulcstanúsítványok műszaki érvényességi idejét

— LC_KA-3: Amennyiben az adattárca-szolgáltató aláírással vagy bélyegzővel lát el egy kulcstanúsítványt, az adott WSCD eszköz vagy kulcstár visszavonási állapotát mindaddig meg kell őriznie, amíg az adott kulcstanúsítványban feltüntetett „key_storage_status.exp” idő el nem telik

— LC_GEN-1: Az adattárca-szolgáltató biztosítja, hogy az adattárcaegység olyan adattárcaegység-tanúsítványokat és kulcstanúsítványokat tudjon megjeleníteni, amelyek „client_status.exp”, illetve „key_storage_status.exp” időpontja az engedélyezési szervernek vagy a hitelesítőadat-kibocsátónak való bemutatás időpontjában a bemutatás időpontjánál legalább 31 nappal későbbi

— *MEGJEGYZÉS*: Ez garantálja azt, hogy a személyazonosítóadat-szolgáltatók a visszavonási láncolatra támaszkodhassanak anélkül, hogy rövid élettartamú személyazonosító adatokat kellene kibocsátaniuk

— LC_GEN-2: Az adattárca-szolgáltató biztosítja, hogy az adattárcaegység a kibocsátás során lekérje a hitelesítőadat-kibocsátó metaadatait

  — LC_GEN_2.1: Ha a metaadatok tartalmaznak egy „preferred_key_storage_status_period” mezőt, az adattárcaegység kulcstanúsítványt küld, amelyben a („key_storage_status.exp” – aktuális idő) – „preferred_key_storage_status_period” érték a lehető legkisebb, de nem negatív. Ha az adattárcaegységnek nem áll rendelkezésére ilyen kulcstanúsítvány, új kulcstanúsítványt kell beszereznie az adattárca-szolgáltatótól, amely megfelel a „key_storage_status.exp” – aktuális idő ≥ „preferred_key_storage_status_period” kritériumnak

  — LC_GEN_2.2: Ha a metaadatok tartalmaznak egy „preferred_client_status_period” mezőt, az adattárcaegység adattárcapéldány-tanúsítványt küld, amelyben a („client_status.exp” – aktuális idő) – „preferred_client_status_period” érték a lehető legkisebb, de nem negatív. Ha az adattárcaegységnek nem áll rendelkezésére ilyen adattárcapéldány-tanúsítvány, új adattárcapéldány-tanúsítványt kell kérnie az adattárca-szolgáltatótól, amely megfelel a „client_status.exp” – aktuális idő ≥ „preferred_client_status_period” kritériumnak

— LC_GEN-3: A személyazonosító adatok műszaki érvényességi idejének az adattárcapéldány-tanúsítvány „client_status.exp”, valamint a kibocsátási folyamat során a személyazonosítóadat-szolgáltatónak küldött kulcstanúsítvány „key_storage_status.exp” érvényességi ideje előtt kell véget érnie

— LC_GEN-4: A 24 óránál hosszabb műszaki érvényességi idejű személyazonosító adatok szolgáltatója a személyazonosító adatok műszaki érvényességi ideje alatt 24 óránként legalább egyszer ellenőrzi mind az adattárcapéldány-tanúsítvány, mind a kibocsátás során kapott kulcstanúsítvány visszavonási állapotát. Bármely tanúsítvány visszavonása esetén a szolgáltató visszavonja a személyazonosító adatokat

e) Visszavonási követelmények

— R_GEN-1: Az adattárca-szolgáltató mind a kulcstanúsítványok, mind az adattárcapéldány-tanúsítványok esetében (az IETF tokenállapot-listában meghatározott) tokenállapot-listákat használja visszavonási mechanizmusként, az OID4VCI szabvány D., illetve E. függelékében meghatározottak szerint

— *MEGJEGYZÉS*: Az állapotlisták jobb méretezhetősége érdekében az adattárca-szolgáltató a következő optimalizálásokat használhatja:

  — Az állapotlista több részre osztása, amennyiben az adattárca-szolgáltatók jelentős számú felhasználóval és kibocsátott tanúsítvánnyal rendelkeznek. Számos felosztási stratégia létezik, például adott méret vagy időszak alapján. A felosztási stratégia az adattárca-szolgáltatók mérlegelési jogkörébe tartozik. Szempontként figyelembe vehető az állapotlista letöltési mérete, illetve a felhasználók magánéletének védelme

  — Több állapotlista fenntartása

  — Az állapotlista tömörítése a méret csökkentése érdekében

— R_WIA-1: Az adattárca-szolgáltató a „client_status.status” állításban ugyanazt az értéket rendelheti az „idx” állításhoz minden, egy adott adattárcaegység által az engedélyezési szervernek megjelenített adattárcapéldány-tanúsítványban. Ezt nevezik „per-issuer reuse” opciónak. E lehetőség választása esetén:

  — R_WIA-1.1: Az adattárcaegységnek számon kell tartania, melyik indexértéket használta az egyes engedélyezési szerverek esetében, amelyekkel korábban kapcsolatba lépett, és ugyanolyan indexértéket tartalmazó adattárcapéldány-tanúsítványt kell kérnie, amikor ismét kapcsolatba lép ugyanazzal az engedélyezési szerverrel

  — R_WIA-1.2: Amennyiben az adattárca-szolgáltatóhoz egy adott indexértéket tartalmazó adattárcapéldány-tanúsítvány iránti kérelem érkezik, az adattárca-szolgáltató az adott indexértéket tartalmazó új adattárcapéldány-tanúsítvány kibocsátása előtt ellenőrzi, hogy a kérelmező adattárcaegység korábban megkapta-e az adott indexértéket

  — R_WIA-1.3: Az adattárcaegység nem használhatja fel újra ugyanazt az indexértéket különböző engedélyezési szerverekkel való interakciókhoz

— *MEGJEGYZÉS*: A „per-issuer reuse” opció használata esetén az adattárca-szolgáltató meg tudja állapítani, hogy az adattárcaegység hány engedélyezési szerverrel lépett kapcsolatba, és milyen gyakran kommunikált velük

— R_WIA-2: Az adattárca-szolgáltató az adatvédelmi szabályzatában dokumentálja, hogy az adattárcapéldány-visszavonáshoz használja-e a „per-issuer reuse” opciót

— R_WIA-3: Amennyiben az adattárca-szolgáltató nem él a „per-issuer reuse” opcióval, friss, nem összekapcsolható indexértéket rendel az általa kibocsátott minden egyes adattárcapéldány-tanúsítványhoz

— R_WIA-4: Amennyiben az adattárcaegységet vissza kell vonni, az adattárca-szolgáltató az adott adattárcaegységhez kapcsolódó valamennyi adattárcapéldány-tanúsítványban visszavonja a „client_status.status” állításban szereplő indexértékeket

— R_WIA-5: Az adattárca-szolgáltató az adattárcapéldány-tanúsítványok állapotlistái méretének meghatározásakor figyelembe veszi az alkalmazási nagyságrendet és a mögöttes architektúrát, gondoskodva arról, hogy az állapotlisták kellően nagy méretűek legyenek a megfeleltethetőség megelőzéséhez és a felhasználók magánéletének védelméhez. Egy állapotlistának lehetőség szerint legalább 10 000 tanúsítványra kell vonatkoznia

— R_KA_1: Az adattárca-szolgáltató a kulcstanúsítványban a „key_storage_status.status” állításhoz az alábbi index-hozzárendelési lehetőségek egyikét választja:

  — 1. lehetőség, ún. „type-shared index” opció, amikor az azonos típusú WSCD eszközben vagy kulcstárban tárolt kulcsokhoz kapcsolódó összes kulcstanúsítvány ugyanazt az indexértéket tartalmazza a „key_storage_status.status” mezőben

  — 2. lehetőség, ún. „per-key-attestion index” opció, amikor az egy-egy WSCD eszközben vagy kulcstárban tárolt kulcsokhoz kapcsolódó kulcstanúsítvány (páros) egyedi indexértéket tartalmaz a „key_storage_status.status” mezőben

— *MEGJEGYZÉS*: Amennyiben az adattárca-szolgáltató az 1. lehetőséget alkalmazza, egyetlen visszavonási intézkedés érvényteleníti az összes adattárcaegységben az érintett típusú valamennyi kulcstanúsítványt. Továbbá, mivel az azonos típusú WSCD eszközhöz vagy kulcstárhoz tartozó valamennyi kulcstanúsítvány egyetlen állapotlista-indexen alapul, a kulcstanúsítványok állapotlistáján szereplő bejegyzések száma az adattárca-szolgáltató által támogatott WSCD eszközök vagy kulcstárolási típusok számát tükrözi, nem pedig a kibocsátott adattárcaegységek számát. Az adattárcapéldány-állapotlisták minimális listaméretét indokoló adatvédelmi megfontolások ezért az 1. lehetőség szerint összeállított kulcstanúsítvány-állapotlistákra nem alkalmazandók, feltéve, hogy elegendő számú adattárcaegység használja ugyanazt a típusú WSCD eszközt vagy kulcstárat

— *MEGJEGYZÉS*: Amennyiben az adattárca-szolgáltató a 2. lehetőséget alkalmazza, az egyes indexértékek az adott kulcstanúsítványban tanúsított konkrét WSCD eszköz vagy kulcstár visszavonási állapotát jelölik

— *MEGJEGYZÉS*: Amennyiben az adattárca-szolgáltató a 2. lehetőséget alkalmazza, egy adott WSCD eszköz vagy kulcstár felhasználói kérésre is visszavonható

— R_KA-2: Amennyiben az adattárca-szolgáltató a 2. lehetőséget alkalmazza, az adattárca-szolgáltató opcionálisan élhet az R_WIA-1 követelményben leírt „per-issuer reuse” opcióval. Ha az adattárca-szolgáltató él ezzel a lehetőséggel, az R_WIA-1–R_WIA-3 követelmények értelemszerűen alkalmazandók

— R_KA-3: Amennyiben az adattárca-szolgáltató a 2. lehetőséget alkalmazza, az adattárca-szolgáltató a kulcstanúsítványok állapotlistái méretének meghatározásakor figyelembe veszi az alkalmazási nagyságrendet és a mögöttes architektúrát, gondoskodva arról, hogy állapotlistái kellően nagy méretűek legyenek a megfeleltethetőség megelőzéséhez és a felhasználók magánéletének védelméhez. Egy állapotlistának lehetőség szerint legalább 10 000 kulcstanúsítványra kell vonatkoznia.

— R_KA-4: Amennyiben az adattárca-szolgáltató az 1. (type-shared index) lehetőséget választja, csak abban az esetben vonhatja vissza a „key_storage_status.status” bejegyzést, ha a WSCD eszköz vagy kulcstár típusa biztonsági szempontból sérülékeny

f) Az aláírási algoritmusokra vonatkozó követelmények

— SA-1: Az adattárcapéldány-tanúsítványok, a kulcstanúsítványok, a kapcsolódó birtoklási igazolások és a tokenállapot-listák aláírásához a következő algoritmusok egyikét kell használni:

— ES256 (ECDSA – SHA-256 és P-256 algoritmussal)

— ES384 (ECDSA – SHA-384 és P-384 algoritmussal)

— ES512 (ECDSA – SHA-512 és P-521 algoritmussal)

— SA-2: Az adattárca-szolgáltató kiválasztja, hogy az SA-1 követelményben említett mely algoritmust használja

— SA-3: Az engedélyezési szervernek vagy a hitelesítőadat-kibocsátónak (az OID4VCI szabványban meghatározottak szerint) támogatnia kell az SA-1 követelményben említett valamennyi algoritmust”

IV. MELLÉKLET

„II. MELLÉKLET

A 8. cikkben említett szabványok jegyzéke

Az ETSI TS 119 472-1 V1.2.1 (2026-02) szabvány 2–6. pontjában meghatározott technikai specifikációk alkalmazandók. Ezek a következő kiigazítással értendők:

1. 2.1. Normative references (Normatív hivatkozások)

   — [16] ETSI EN 319 412-1 V1.6.1 (2025-06): „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures" (Elektronikus aláírások és infrastruktúrák [ESI]. Tanúsítványprofilok. 1. rész: Áttekintés és közös adatszerkezetek)

   — [17] ETSI TS 119 412-6 V1.1.1 (2025-09): „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers" (Elektronikus aláírások és bizalmi infrastruktúrák [ESI]. Tanúsítványprofilok. 6. rész: 6: A PID-, tárca-, EAA-, QEAA- és PSBEAA-szolgáltatókra érvényes tanúsítványprofil-követelmények)

   — [25] IETF tokenállapot-lista (TSL), draft-ietf-oauth-status-list-20: „Token Status List" (tokenállapot-lista), 2026. április 20.

2. 4.2.11.1. General requirements (Általános követelmények)

   — EAA-4.2.11.1-06: A személyazonosító adatok, a minősített elektronikus attribútumtanúsítványok vagy a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok esetében állapotelem használata esetén az utóbbinak csak azt kell jeleznie, hogy a tanúsítványt visszavonták-e vagy sem, és az nem támogathat más állapotértéket, mint például felfüggesztést

   — EAA-4.2.11.1-06.1: Amennyiben egy tanúsítvány visszavonásra kerül, a visszavonásnak véglegesnek kell lennie

3. 4.2.13. EAA short-lived (Rövid élettartamú elektronikus attribútumtanúsítványok)

   — EAA-4.2.13-03: Amennyiben 24 órás vagy annál rövidebb érvényességi idejű, rövid élettartamú elektronikus attribútumtanúsítványok kerülnek kibocsátásra, nincs szükség visszavonásra

4. 4.6.3. Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA) (A hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott uniós elektronikus attribútumtanúsítványokra [PuB-EAA] vonatkozó követelmények)

   — PuB-EAA-4.6.2-03: érvénytelen

   — Pub-EAA-4.6.2-04: érvénytelen

   — PuB-EAA-4.6.3-03: A PuB-EAA digitális aláírásának tartalmaznia kell a PuB-EAA digitális aláírását támogató minősített tanúsítványt

   — PuB-EAA-4.6.3-04: A PuB-EAA digitális aláírását támogató minősített tanúsítványnak meg kell felelnie az ETSI TS 119 412-6 szabvány 1.1.1. verziója 8. szakaszában foglalt követelményeknek, és tartalmaznia kell az ETSI EN 319 412-5 szabvány 2.5.1. verziójában meghatározott QcType qcStatement kiterjesztést, amelynek id-etsi-qct-eidaspsbeaa értéke a következőképpen kerül meghatározásra:

     id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 }– A 910/2014/EU rendelet 3. cikkének 46. pontjában említett közigazgatási szerv minősített elektronikus aláírását vagy minősített elektronikus bélyegzőjét alátámasztó, a 45f. cikk (1) bekezdésének b) pontjában említett tanúsítvány

5. 5.2.10.1. General requirements (Általános követelmények)

   — EAA-5.2.10.1-04: érvénytelen

   — EAA-5.2.10.1-05: érvénytelen

   — EAA-5.2.10.1-06: A status tag tartalmazhatja a status_list tagot az IETF draft-ietf-oauth-status-list-20 [25] 6.2. szakaszában meghatározottak szerint

   — EAA-5.2.10.1-07: érvénytelen

— EAA-5.2.10.1-08: érvénytelen

— EAA-5.2.10.1-09: érvénytelen

— EAA-5.2.10.1-10: érvénytelen

— EAA-5.2.10.1-11: érvénytelen

— EAA-5.2.10.1-12: érvénytelen

6. 6.2.10.1. General requirements (Általános követelmények)

— EAA-6.2.10.1-01: Amennyiben az ISO/IEC mdoc szabványnak megfelelő elektronikus attribútumtanúsítvány az EAA-6.2.10.1-02.2. pont szerinti tanúsítvány-állapotlista mechanizmust vagy az EAA-6.2.10.1-02.3. pont szerinti tanúsítvány-visszavonási lista mechanizmust alkalmazza, a mobileszköz-biztonsági objektumának (MSO) tartalmaznia kell az EAA-6.2.10.1-17. pontban meghatározott állapotstruktúrát, amely MSO-visszavonási információkat is tartalmaz

— EAA-6.2.10.1-01.1: Az azonosítólista-mechanizmus alkalmazásakor az állapotelemnek tartalmaznia kell az EAA-6.2.10.1-11. pont szerinti identifier_list elemet

— EAA-6.2.10.1-01.2: Az állapotlista-mechanizmus alkalmazásakor az állapotelemnek tartalmaznia kell az EAA-6.2.10.1–13-ban meghatározott status_list elemet

— *MEGJEGYZÉS*:

  — Az állapotstruktúra hivatkozást tartalmaz egy MSO visszavonási listára

  — Az MSO visszavonási lista egy COSE_Sign1 struktúra, amely jelzi, hogy egy adott MSO visszavonásra került-e vagy sem

  — Az állapotstruktúra minden olyan információt tartalmaz, amelyre az adattárca-igénybevevőnek szüksége van annak megállapításához, hogy az MSO visszavonási lista hiteles-e

— EAA-6.2.10.1-02: A személyazonosító adatok szolgáltatója, a minősített elektronikus attribútumtanúsítványok szolgáltatója, illetve a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok szolgáltatója az alábbi módszerek egyikét alkalmazza a személyazonosító adatok, a minősített elektronikus attribútumtanúsítványok, illetve a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok visszavonására:

— EAA-6.2.10.1-02.1: Amennyiben a szolgáltató 24 órás vagy annál rövidebb érvényességi idejű, rövid élettartamú elektronikus attribútumtanúsítványokat bocsát ki, nincs szükség visszavonásra

— EAA-6.2.10.1-02.2: A visszavonási információk állapotlistaként történő kódolásához a tanúsítvány-állapotlista mechanizmus használandó

— EAA-6.2.10.1-02.2.1: Az állapotlista mechanizmus az alapján vonja vissza az MSO-t, hogy az MSO-ban a kibocsátó által meghatározott bitpozícióban található bit igaz értékkel rendelkezik-e az állapotlistában

— EAA-6.2.10.1-02.2.2: Az állapotlista mechanizmus leírását a tokenállapot-listára vonatkozó előírás (draft-ietf-oauth-status-list-20) tartalmazza

— EAA-6.2.10.1-02.3: A visszavonási információk azonosítólistaként történő kódolásához a tanúsítvány-visszavonási lista mechanizmus használandó

— EAA-6.2.10.1-02.3.1: Az azonosítólista mechanizmus az alapján vonja vissza az MSO-t, hogy az MSO kibocsátó által meghatározott azonosítója szerepel-e az azonosítólistán

— EAA-6.2.10.1-02.3.2: Az EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 és EAA-6.2.10.1-11 előírás az azonosítólista mechanizmust írja le, a tokenállapot-lista specifikáció követelményei alapján, az állapotlista és az azonosítólista mechanizmus közös tulajdonságait is beleértve

— EAA-6.2.10.1-03: Amennyiben a személyazonosító adatok, a minősített elektronikus attribútumtanúsítványok vagy a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok esetében állapotelem használatára kerül sor, kizárólag a „revoked” (visszavont) állapot használható

— EAA-6.2.10.1-03.1: Állapotlista esetében ez azt jelenti, hogy csak a tokenállapot-lista specifikációjában meghatározott „valid” (érvényes) és „invalid” (érvénytelen) értékek használhatók

— EAA-6.2.10.1-03.2: Azonosítólista esetében csak visszavont MSO-k kerülhetnek fel az azonosítólistára, szemben az ideiglenesen felfüggesztett MSO-kkal

— EAA-6.2.10.1-04: Amennyiben egy MSO visszavonásra kerül, az MSO visszavonásának véglegesnek kell lennie

— EAA-6.2.10.1-05: Az MSO visszavonási lista ellenőrzése az adattárca-igénybevevő esetében opcionális, és adott esetben az ellenőrzésnek meg kell felelnie a tokenállapot-lista specifikációjában meghatározott ellenőrzési követelményeknek és az EAA-6.2.10.1-01 követelményben meghatározott állapotstruktúra specifikációnak

— EAA-6.2.10.1-05.1: Amennyiben az adattárca-igénybevevőnek szüksége van arra, hogy ellenőrizni tudja a személyazonosító adatok vagy az elektronikus attribútumtanúsítványok visszavonási állapotát, támogatnia kell mind a tanúsítványállapot-lista mechanizmust, mind a tanúsítvány-visszavonási lista mechanizmust, az EAA-6.2.10.1-02 követelménynek megfelelően

— EAA-6.2.10.1-06: Az MSO-ban az identifier_list, illetve a status_list tartalmazhatja a tanúsítványelemet

— EAA-6.2.10.1-06.1: Amennyiben található ott tanúsítványelem, annak tartalmaznia kell egy tanúsítványt, amelyben megtalálható az MSO visszavonási lista struktúrájának x5chain elemében a legmagasabb szintű tanúsítványt aláírással vagy bélyegzővel ellátó nyilvános kulcs

— EAA-6.2.10.1-06.1.1: Az adattárca-igénybevevő példánya ezt a tanúsítványt bizalmi horgonyként használja az MSO visszavonási listájában az x5chain elem ellenőrzéséhez

— EAA-6.2.10.1-06.2: Amennyiben nincs jelen tanúsítványelem, az MSO visszavonási lista struktúrájának x5chain elemében található legfelsőbb szintű tanúsítványt aláírással vagy bélyegzővel kell ellátni az MSO x5chain elemében szereplő tanúsítvány aláírására vagy bélyegzővel való ellátására használt tanúsítvánnyal

— EAA-6.2.10.1-06.2.1: Az adattárca-igénybevevő példánya ezt a tanúsítványt bizalmi horgonyként használja az MSO visszavonási listájában az x5chain elem ellenőrzéséhez

— EAA-6.2.10.1-07: Az MSO visszavonási listáját a tokenállapot-lista specifikációjának megfelelően, CWT formátumú állapotlista-tokenként kell végrehajtani

— EAA-6.2.10.1-08: Az azonosítólista és állapotlista mechanizmushoz kapcsolódó MSO visszavonási lista esetében az alábbi követelmények alkalmazandók:

  — szerepelnie kell az exp állításnak

  — szerepelhet a ttl állítás

  — az aggregation_uri állítás szerepelhet az IdentifierList vagy StatusList állításban, és a személyazonosító adatok szolgáltatója, a minősített elektronikus attribútumtanúsítványok szolgáltatója vagy a hiteles

forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok szolgáltatója az aggregation_uri állítást használhatja a tokenállapot-lista specifikációja szerinti aggregálási mechanizmus támogatott voltának jelzésére

— a CWT állításnak COSE_Sign1 objektumnak kell lennie, amely az alábbi aláírási algoritmusok egyikét használja az aláírás számításához:

a) „ES256” (ECDSA, NIST P-256 görbével és SHA-256 algoritmussal);

b) „ES384” (ECDSA, NIST P-384 görbével és SHA-384 algoritmussal);

c) „ES512” (ECDSA, NIST P-521 görbével és SHA-512 algoritmussal);

d) „ESB256” (ECDSA, brainpoolP256r1 görbével és SHA-256 algoritmussal);

e) „ESB384” (ECDSA, brainpoolP384r1 görbével és SHA-384 algoritmussal);

f) „ESB512” (ECDSA, brainpoolP512r1 görbével és SHA-512 algoritmussal);

— a CWT-nek tartalmaznia kell az x5chain elemet az MSO visszavonási lista aláírásának ellenőrzésére szolgáló tanúsítványt vagy a tanúsítványláncot tartalmazó védett fejlécben

— a tokenállapot-listára vonatkozó specifikációban meghatározott objektumazonosító kiterjesztett kulcshasználata használható az állapotlista és az azonosítólista aláírási tanúsítványához, és az adattárca-igénybevevői példányok támogathatják a tokenállapot-lista specifikációjában meghatározott objektumazonosító kiterjesztett kulcshasználatát; az objektumazonosító esetében pedig a minősített elektronikus attribútumtanúsítványok szolgáltatója vagy a közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványok szolgáltatója nem teheti kritikussá a kiterjesztett kulcshasználat mezőt a tokenállapot-listára vonatkozó specifikációban meghatározott, kiterjesztett kulcshasználatú OID alkalmazásakor

— EAA-6.2.10.1-09: A tokenállapot-lista specifikáció követelményeitől eltérve az azonosítólista mechanizmusra a következő követelmények vonatkoznak:

— a type állítás értéke legyen „application/identifierlist+cwt”

— a StatusList állítás nem szerepelhet a CWT állításkészletben

— az EAA-6.2.10.1-11. pontban meghatározott IdentifierList struktúrának állításként szerepelnie kell a CWT állításkészletben a 65530 kulcs használatával

— EAA-6.2.10.1-10: Az IdentifierList struktúra CBOR struktúra, a következő CDDL-lel:

```
IdentifierList = {

    'identifiers': { * Identifier => IdentifierInfo },

    ? 'aggregation_uri': Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: Amennyiben az IdentifierList listán szerepel az azonosító, az az MSO, amely az állapotelemben tartalmazza az azonosítót, visszavonásra kerül

— EAA-6.2.10.1-10.2: Az Aggregation_uri állítást a tokenállapot-lista specifikációjának 9.2. szakasza írja le

— EAA-6.2.10.1-10.3: Az azonosítólista tartalomtípusa legyen „application/identifierlist+cwt”, a tokenállapot-lista specifikációjának 8.2. szakaszában meghatározott követelmények szerint

— EAA-6.2.10.1-11: Az MSO-ban szereplő identifier_list elemre a következő követelmények vonatkoznak (lásd EAA-6.2.10.1-17)

— EAA-6.2.10.1-11.1: Az identifier_list elem CBOR struktúra, a következő CDDL-lel:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: Annak érdekében, hogy az azonosító különböző megjelenítései ne legyenek összekapcsolhatók, minden MSO esetében egyedi azonosítót kell használni

— EAA-6.2.10.1-12: Az állapotlistára a következő követelmények vonatkoznak:

  — EAA-6.2.10.1-12.1: A StatusList struktúra bitek eleménél az 1 értéket kell megadni

— EAA-6.2.10.1-13: Az MSO-ban szereplő status_list elemre a következő követelmények vonatkoznak (lásd EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: A status_list elemnek meg kell felelnie a StatusListInfo struktúrára vonatkozóan a tokenállapot-lista specifikációjában meghatározott követelményeknek, és hozzá kell adni az EAA-6.2.10.1-06 pont szerinti opcionális tanúsítványelemet

  — EAA-6.2.10.1-13.2: Annak érdekében, hogy az állapotindex különböző megjelenítései ne legyenek összekapcsolhatók, az állapotindex és az URI kombinációjának minden MSO esetében egyedinek kell lennie

— EAA-6.2.10.1-14: Az adattárca-szolgáltatónak az EAA-6.2.10.1-02. pontban meghatározott módszerek közül a másodikat (EAA-6.2.10.1-02.2) vagy a harmadikat (EAA-6.2.10.1-02.3) kell alkalmaznia az adattárcapéldány-tanúsítvány (WIA) vagy a kulcstanúsítvány (KA) visszavonásának céljára

— EAA-6.2.10.1-15: Az adattárca-szolgáltató az adattárca-megoldásban az EAA-6.2.10.1-02. pontban leírt tanúsítvány-visszavonási mechanizmusokat alkalmazza

— EAA-6.2.10.1-16: A személyazonosítóadat-szolgáltató és az elektronikus attribútumtanúsítványok szolgáltatója az adattárcapéldány-tanúsítványok (WIA) vagy a kulcstanúsítványok (KA) visszavonási állapotának ellenőrzése céljából egyaránt támogatja az EAA-6.2.10.1-02. pont szerinti tanúsítványállapot-lista mechanizmust, illetve tanúsítvány-visszavonási lista mechanizmust

— EAA-6.2.10.1-17: Az MSO-ban az állapotstruktúra CBOR struktúra, a következő CDDL-lel:

Status = {

? 'identifier_list' : IdentifierListInfo,

? 'status_list' : StatusListInfo,

* tstr => RFU

}”

V. MELLÉKLET

„III. MELLÉKLET

A 10. cikkben említett technikai specifikációk

— Technikai specifikációk:

  — Az ETSI TS 119 472-3 V1.1.1 (2026-03) 4.2.5. pontja.”

VI. MELLÉKLET

Az (EU) 2024/2979 rendelet IV. melléklete a következőképpen módosul:

1. Az 1. pont helyébe a következő szöveg lép:

„1. Kötelező aláírási vagy bélyegzőformátum:

a) PAdES (PDF Advanced Electronic Signature), a következő szabvány szerint: ETSI EN 319 142-1 V1.2.1 (2024-01); 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. A 3. pont helyébe a következő szöveg lép:

„3. Alkalmazásprogramozási felület:
ETSI TS 119 432 v1.3.1 (2026-03), 6.4.3., A.6., A.7. és A.8. pont.”

VII. MELLÉKLET

„VI. MELLÉKLET

Az európai digitális személyiadat-tárca bizalmi jegyének színes változata



”

VIII. MELLÉKLET

„VII. MELLÉKLET

Az európai digitális személyiadat-tárca bizalmi jegyének fekete-fehér változata



”

IX. MELLÉKLET

„VIII. MELLÉKLET

Az európai digitális személyiadat-tárca bizalmi jegyének adatai

Adatok	Leírás	Kódolás	Állapot
TrustMarkResourceURL	Az európai digitális személyiadat-tárca bizalmi védjegyéhez tartozó grafikai elemek és az adattárca felhasználói felületén található felhasználói információforrások URL-címe.	URL	Kötelező
ListOfCertifiedWalletsURL	Az uniós tanúsított adattárca-megoldások (EU) 2025/849 bizottsági végrehajtási rendelet ([1]) szerinti nyilvános jegyzékének URL-címe.	URL	Kötelező
ListOfCertifiedWalletsQRCode	A ListOfCertifiedWalletsURL adatait tartalmazó QR-kód.	ISO-8859-1 Byte mode QR code	Opcionális
WalletSolutionInfoPageURL	A tanúsított adattárca-megoldások listáját tartalmazó oldalon szereplő tanúsított adattárca-megoldás információs oldalának URL-címe a ListOfCertifiedWalletsURL URL-címről, „?” karakterrel és az adattárca-megoldás WalletSolutionID azonosítójával kiegészítve.	URL	Kötelező
WalletSolutionInfoPageQRCode	A WalletSolutionInfoPageURL adatait tartalmazó QR-kód.	ISO-8859-1 Byte mode QR code	Opcionális
WalletVerifierToolURL*	Az adattárca-ellenőrző eszköz azon */.well-known/openid-credential-issuer* végpontjára mutató URL-cím, amelyet a hitelesítőadat-szolgáltató metaadatainak lekérdezéséhez használnak.	URL	Opcionális

([1]) A Bizottság (EU) 2025/849 végrehajtási rendelete (2025. május 6.) a 910/2014/EU európai parlamenti és tanácsi rendeletnek a tanúsított európai digitális személyiadat-tárcák listájával kapcsolatban a Bizottság és az együttműködési csoport részére benyújtandó információk tekintetében történő alkalmazására vonatkozó szabályok megállapításáról (HL L, 2025/849, 2025.5.7., ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).”

X. MELLÉKLET

Az (EU) 2024/2980 végrehajtási rendelet II. melléklete a következőképpen módosul:

1. A II. melléklet 1. szakaszának 1.i) pontja helyébe a következő szöveg lép:

„i) egy vagy több, az ETSI EN 319 412-2 V2.4.1 (2025-06) vagy az ETSI EN 319 412-3 V1.3.1 (2023-09) szabványnak megfelelő tanúsítvány, amely felhasználható a nyilvántartó által a nyilvántartási adatokon létrehozott aláírás vagy bélyegző ellenőrzésére, és amelynek esetében a hitelesített személyazonosító adatok között szerepel a nyilvántartó neve és adott esetben nyilvántartási száma, a c) és d) pontban előírtak szerint."

2. A II. melléklet 2. szakaszának 1.h) pontja helyébe a következő szöveg lép:

„h) egy vagy több, az ETSI EN 319 412-2 V2.4.1 (2025-06) vagy az ETSI EN 319 412-3 V1.3.1 (2023-09) szabványnak megfelelő tanúsítvány, amely felhasználható az adattárca-szolgáltató által kibocsátott adattárcaegység-tanúsítványok hitelesítésére és érvényesítésére, és amelynek esetében a hitelesített személyazonosító adatok között szerepel az adattárca-szolgáltató neve és adott esetben nyilvántartási száma, az a) és b) pontban előírtak szerint;".

3. A II. melléklet 3. szakaszának 1.h) pontja helyébe a következő szöveg lép:

„h) egy vagy több, az ETSI EN 319 412-2 V2.4.1 (2025-06) vagy az ETSI EN 319 412-3 V1.3.1 (2023-09) szabványnak megfelelő tanúsítvány, amely felhasználható a személyazonosítóadat-szolgáltató által az általa szolgáltatott személyazonosító adatokon létrehozott aláírás vagy bélyegző ellenőrzésére, és amelynek esetében a hitelesített személyazonosító adatok között szerepel a személyazonosítóadat-szolgáltató neve és adott esetben nyilvántartási száma, az (a) és (b) pontban előírtak szerint."

4. A II. melléklet 4. szakaszának 1.g) pontja helyébe a következő szöveg lép:

„g) egy vagy több, az ETSI EN 319 412-2 V2.4.1 (2025-06) vagy az ETSI EN 319 412-3 V1.3.1 (2023-09) szabványnak megfelelő tanúsítvány, amely felhasználható az adattárca-igénybevevői hozzáférési tanúsítványok szolgáltatója által az általa az adattárca-igénybevevőknek kiadott hozzáférési tanúsítványon létrehozott aláírás vagy bélyegző ellenőrzésére, adott esetben azokkal az információkkal együtt, amelyek lehetővé teszik az adattárca-igénybevevői hozzáférési tanúsítványok megkülönböztetését más tanúsítványoktól."

5. A II. melléklet a következő 5. szakasszal egészül ki:

„5. Az adattárca-igénybevevői nyilvántartási tanúsítványok szolgáltatóira vonatkozó információk bejelentése

1. A tagállamok a Bizottság rendelkezésére bocsátják az adattárca-igénybevevői nyilvántartási tanúsítványok szolgáltatóira vonatkozó alábbi információkat:

a) az adattárca-igénybevevői nyilvántartási tanúsítványok szolgáltatójának neve;

b) adott esetben az adattárca-igénybevevői nyilvántartási tanúsítványok szolgáltatójának nyilvántartási száma;

c) az adattárca-igénybevevői nyilvántartási tanúsítványok szolgáltatójának letelepedési helye szerinti tagállam;

d) az adattárca-igénybevevői nyilvántartási tanúsítványok szolgáltatójának kapcsolattartási e-mail-címe és telefonszáma (az általa az adattárca-igénybevevőknek biztosított nyilvántartási tanúsítványokkal kapcsolatos ügyek kezelése céljából);

e) adott esetben az adattárca-igénybevevői nyilvántartási tanúsítványok szolgáltatója weboldalának URL-je, amely további információkat tartalmaz a szolgáltatóról és az általa az adattárca-igénybevevőknek biztosított nyilvántartási tanúsítványokról;

f) annak a weboldalnak az URL-címe, ahol az adattárca-igénybevevői nyilvántartási tanúsítványok kiadására és használatára vonatkozó szabályzat és feltételek találhatók;

g) egy vagy több, az ETSI EN 319 412-2 V2.4.1 (2025-06) vagy az ETSI EN 319 412-3 V1.3.1 (2023-09) szabványnak megfelelő tanúsítvány, amely felhasználható az adattárca-igénybevevői nyilvántartási tanúsítványok szolgáltatója által az általa az adattárca-igénybevevőknek kiadott nyilvántartási tanúsítványokon létrehozott aláírás vagy bélyegző ellenőrzésére, adott esetben azokkal az információkkal együtt, amelyek lehetővé teszik az adattárca-igénybevevői nyilvántartási tanúsítványok megkülönböztetését más tanúsítványoktól.

2. Az 1. pontban említett információkat az adattárca-igénybevevői nyilvántartási tanúsítványok minden egyes szolgáltatója esetében külön meg kell adni.”

XI. MELLÉKLET

„I. MELLÉKLET

A 4. cikkben említett protokollok és interfészek

Az ETSI TS 119 472-3 V1.1.1 (2026-03) technikai specifikáció alkalmazandó, a következő kiigazításokkal:

1. 4.1. General requirements (Általános követelmények)

   — GEN-REQ-4.1-05: érvénytelen

   — MEGJEGYZÉS: érvénytelen

2. 4.2.3. Provision of registration certificates of PID/EAA Provider to EUDI Wallet (PID-/EAA-szolgáltatói nyilvántartási tanúsítványok kiállítása az európai digitális személyiadat-tárcák számára)

   — ISS-MDATA-REG_CERT-4.2.3-04: Az issuer_info tömbparaméter egyik elemének tartalmaznia kell a PID-/EAA-szolgáltató nyilvántartási tanúsítványát

   — ISS-MDATA-REG_CERT-4.2.3-07: érvénytelen

   — ISS-MDATA-REG_CERT-4.2.3-08: érvénytelen

   — ISS-MDATA-REG_CERT-4.2.3-09: érvénytelen

   — ISS-MDATA-REG_CERT-4.2.3-10: érvénytelen

   — ISS-MDATA-REG_CERT-4.2.3-11: érvénytelen

   — ISS-MDATA-REG_CERT-4.2.3-12: érvénytelen

   — ISS-MDATA-REG_CERT-4.2.3-13: érvénytelen

3. 4.2.4.2. ARF pre-defined PID/EAA reuse policy (ARF előre meghatározott PID-/EAA-újrafelhasználási politika)

   — ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Amennyiben az id tag értéke „arf_annex_ii”, és a „details” címkéhez rendelt tömb tartalmazza a „once_only” vagy a „per-relying-party” értéket, akkor a „details” címkéhez rendelt tömböt tartalmazó JSON objektumnak egy, a „reissue_trigger_unused” címkéhez hozzárendelt JSON számot is tartalmaznia kell

4. Az A. melléklet nem alkalmazandó.”

XII. MELLÉKLET

„II. MELLÉKLET

Az 5. cikkben említett technikai specifikációk

Az ISO/IEC 18013-7:2025 szabvány C. mellékletében foglalt technikai specifikáció alkalmazandó.

Az ETSI TS 119 472-2 V1.2.1 (2026-03) szabvány 4.1., 4.2., 5. és 6. pontjában foglalt technikai specifikációk alkalmazandók, a következő kiigazításokkal, beleértve egy új, 4.3. számú szakasz beillesztését:

1. 1. Scope (Alkalmazási kör)

— A jelen dokumentum két protokollprofilt határoz meg, amelyek lehetővé teszik az igénybevevők (Relying Parties, a továbbiakban: RP) számára EAAP-ok vagy személyi azonosító adatok (Personal Identification Data, a továbbiakban: PID) kérését az európai digitális személyiadat-tárcától, illetve az európai digitális személyiadat-tárca számára a kért EAAP-ok/PID adatok elküldését az RP-nek. Mindkét profil két átviteli mechanizmust támogat, nevezetesen: API-n keresztüli és nem API-n keresztüli átvitelt, az alábbiak szerint:

a) A profilok a következőkre épülnek:

— ISO/IEC 18013-5 [10] csak a nem API-n keresztüli átviteli mechanizmus esetében, valamint

— az ISO/IEC 18013-7 [16] szabvány C. melléklete az API-n keresztüli átviteli mechanizmus esetében

Ennek a profilnak az elnevezése ISO/IEC-mdoc profil, és meghatározását e dokumentum 5. pontja tartalmazza;

b) A profilok a következőkre épülnek:
OpenID4VC-HAIP [11] mind az API-n keresztüli és a nem API-n keresztüli átviteli mechanizmusok esetében, a következők szerint:

— a [11] 5., 5.1., 5.3., 7. és 8. szakasza a Redirects-en vagy nem API-n keresztül közvetített átviteli mechanizmusok esetében, valamint

— a [11] 5., 5.2., 5.3., 7. és 8. szakasza az API-n keresztüli átviteli mechanizmus esetében

Ennek a profilnak az elnevezése OpenID4VC-HAIP profil, és meghatározását e dokumentum 6. pontja tartalmazza.

2. 2.1. Normative references (Normatív hivatkozások)

— [15] ISO 639: „Language code” (Nyelvkód)

— [16] ISO/IEC 18013-7:2025 „Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions” (Személyi azonosítás – ISO – megfelelő vezetői engedély – 7. rész: Mobil vezetői engedély (mDL) beépülő modul funkciói)

3. 4.1. EAAP implementation based on SD-JWT VC (Az SD-JWT VC formátumon alapuló EAAP-implementáció)

— EAAP-SD-JWT VC-04: érvénytelen

4. 4.2. EAAP implementation based on ISO/IEC-mdoc (Az ISO/IEC-mdoc formátumon alapuló EAAP-implementáció)

— EAAP-ISO/IEC-mdoc-01: érvénytelen

— Note2: érvénytelen

— EAAP-ISO/IEC-mdoc-02: érvénytelen

5. 4.3. EAAP implementation with mediating API (EAAP-implementáció közvetítő API-val)

— EAAP-API-GEN-01: Az európai digitális személyiadat-tárca olyan közvetítő API-t támogat, amely támogatja a [11] 5.2. szakaszában és a [16] C. mellékletében meghatározott mindkét protokollt

— *MEGJEGYZÉS*: Amennyiben az eszköz, amelyre az európai digitális személyiadat-tárcát telepítették, nem támogatja mindkét protokollt, ez a követelmény nem teljesíthető, és meg nem felelést eredményez, mivel az alapul szolgáló operációs rendszerek és böngészők nem alkalmazzák a szükséges interoperabilitási funkciókat

— EAAP-API-GEN-02: Az európai digitális személyiadat-tárcának támogatnia kell a közvetítő API-t legalább az (EU) 2025/1569 végrehajtási rendeletben meghatározott rendszerkatalógusban regisztrált PID-k és EAA-típusok, valamint legalább az (EU) 2024/2979 végrehajtási rendelet II. mellékletében meghatározott valamennyi formátum esetében

— *1. MEGJEGYZÉS*: Amennyiben az alapul szolgáló operációs rendszer, böngésző, közvetítő API-k vagy bármely más, az európai digitális személyiadat-tárca által nem befolyásolható technikai réteg korlátozza, szűri, előválogatja vagy más módon korlátozza a tanúsítványformátumokat, valamint a rendszerek katalógusában regisztrált PID- és EAA-típusokat, ez a követelmény nem teljesíthető. Amennyiben az említett korlátozás megakadályozza az európai digitális személyiadat-tárcát abban, hogy támogassa a nyilvántartásba vett tanúsítványtípust vagy -formátumot, az ebből eredő meg nem felelés annak tudható be, hogy az alapul szolgáló operációs rendszerek, böngészők, közvetítő API-k vagy más releváns technikai rétegek nem biztosítják a szükséges interoperabilitási funkciókat

6. 4.4. Wallet-relying party validation and overasking checks (Az adattárca-igénybevevő érvényesítési és túlzott információkérési ellenőrzései)

— WRP-VALIDATION-01: Az európai digitális személyiadat-tárca érvényesíti a kérelemben kapott adattárca-igénybevevői nyilvántartási tanúsítványt, mielőtt a kért személyazonosító adatokat vagy elektronikus attribútumtanúsítványokat megjeleníti jóváhagyásra az adattárca-felhasználónak

— WRP-VALIDATION-02: Amennyiben az adattárca-igénybevevői nyilvántartási tanúsítvány érvényesítése sikertelen – beleértve azt az esetet is, amikor a tanúsítvány lejárt, visszavonták, nem az adattárca-igénybevevői nyilvántartási tanúsítványok érvényes megbízható szolgáltatója bocsátotta ki, hibás vagy kriptográfiailag nem ellenőrizhető –, az európai digitális személyiadat-tárcának figyelmeztetnie kell az adattárca-felhasználót arra, hogy az adattárca-igénybevevőt nem lehetett érvényesíteni, és az nem mutathatja be a kérelmet sikeresen érvényesítettként. Az adattárca-felhasználónak kifejezetten jóvá kell hagynia az igénybe vevő fél kérését. A hallgatólagos beleegyezés vagy az előre bejelölt jelölőnégyzetek nem elegendőek a kifejezett jóváhagyáshoz

— WRP-VALIDATION-03: Az adattárca-szolgáltató az általa végzett kockázatelemzés és a biztonsági szabályzata alapján meghatározza, hogy az adattárca-felhasználó megkerülhet-e adott meghiúsult érvényesítési ellenőrzéseket, és ha igen, milyen feltételek mellett teheti ezt

— WRP-OVERASKING-01: Az európai digitális személyiadat-tárca összehasonlítja az adattárca-igénybevevő által kért tanúsítványokat és attribútumokat az adattárca-igénybevevő nyilvántartási tanúsítványában szereplő, nyilvántartásba vett tanúsítványokkal és attribútumokkal

— WRP-OVERASKING-02: Amennyiben az adattárca-igénybevevő olyan személyazonosító adatokat vagy elektronikus attribútumtanúsítványokat, illetve vagy állításokat igényel, amelyekre nem terjed ki az adattárca-igénybevevői nyilvántartási tanúsítvány, az európai digitális személyiadat-tárcának az adatok közlése előtt egyértelműen figyelmeztetnie kell az adattárca-felhasználót. A figyelmeztetésben fel kell tüntetni, hogy az adattárca-igénybevevő több információt kér, mint amennyi a nyilvántartásában szerepel. Az adattárca-felhasználónak kifejezetten jóvá kell hagynia az igénybe vevő fél kérését. A hallgatólagos beleegyezés vagy az előre bejelölt jelölőnégyzetek nem elegendőek a kifejezett jóváhagyáshoz

— WRP-OVERASKING-03: Az adattárca-szolgáltató az általa végzett kockázatelemzés, a biztonsági szabályzata és az alkalmazandó jog alapján meghatározza, hogy az adattárca-felhasználó az említett figyelmeztetés ellenére folytathatja-e a műveletet, hogy csak a kért adatoknak a nyilvántartási tanúsítványban szereplő része közölhető-e, vagy hogy el kell-e utasítani a kérést

7. 5.1. Introduction (Bevezetés)

— Az 5. szakasz és annak alpontjai meghatározzák azon protokoll profilját, amely lehetővé teszi az RP számára az EAAP-ok/PID adatok lekérését az európai digitális személyiadattárcától, illetve az európai digitális személyiadattárca számára a kért EAAP-ok/PID adatok elküldését, vagy az ISO/IEC 18013-5 [10] szabványra épülő, nem API-n keresztüli átviteli mechanizmus, vagy az ISO/IEC 18013-7 [16] szabvány C. mellékletére épülő, API-n keresztüli átviteli mechanizmus használatával, az ISO/IEC 18013-5 [10] szabvány szerinti, megfelelően beágyazott adatstruktúrák formájában

— Az 5. szakasz többi része a következőképpen épül fel:

  — az 5.2. pont a profil és az átviteli mechanizmusok RP-k és európai digitális személyiadat-tárcák általi támogatására vonatkozó követelményeket határozza meg

  — az 5.3. pont a nem API-n keresztül közvetített átviteli mechanizmusra vonatkozó egyedi követelményeket határozza meg

  — az 5.4. pont és alpontjai az API-n keresztüli átviteli mechanizmusra vonatkozó egyedi követelményeket határozza meg

8. 5.2. Requirements on EUDI Wallet and RP support (Az európai digitális személyiadat-tárca és az RP általi támogatásra vonatkozó követelmények)

— ISO/IEC 18013-SUPPORT-01: Az adattárcaegységek, a PID szolgáltatók, a tanúsítványszolgáltatók, az adattárca-szolgáltatók és az igénybevevők nem támogathatják az ISO/IEC 18013-5 [10] szabványban leírt szerverlekérdezést PID vagy tanúsítványattribútum kérése és bemutatása céljára

— ISO/IEC 18013-SUPPORT-02: Az európai digitális személyiadat-tárcának meg kell felelnie az e dokumentum 5.3. és 5.4. pontjában meghatározott követelményeknek

— ISO/IEC 18013-SUPPORT-04: Az igénybe vevő félnek alkalmaznia kell az e dokumentum 5.4. pontjában meghatározott profilt

9. 5.3.2. ISO/IEC-mdoc EAAP Request contents (ISO/IEC-mdoc EAAP-kérelem tartalma)

— ISO/IEC 18013-5-REQ-04: Az európai digitális személyiadat-tárcáknak küldött eszközkéréseknek tartalmazniuk kell a [10] szabvány 8.3.2.1.2.1. pontjában meghatározott „requestInfo” kulcsértékpárt. Az értékpár értékének RequestInfo típusúnak kell lennie

— ISO/IEC 18013-5-REQ-05: A RequestInfo típusnak meg kell felelnie a CDDL alábbi meghatározásának.

```
RequestInfo = {

    'euWrprc': bstr ; nyilvántartási tanúsítványt tartalmaz (lásd az alábbi követelményeket)

}
```

— ISO/IEC 18013-5-REQ-06: Az említett requestInfo tagnak tartalmaznia kell egy „euWrprc” címkével ellátott tagot

— ISO/IEC 18013-5-REQ-07: Az „euWrprc” értéke egy CBOR kódolású nyilvántartási tanúsítvány

— ISO/IEC 18013-5-REQ-08: érvénytelen

— 3. MEGJEGYZÉS: érvénytelen

— ISO/IEC 18013-5-REQ-09: érvénytelen

— ISO/IEC 18013-5-REQ-10: érvénytelen

— ISO/IEC 18013-5-REQ-11: érvénytelen

10. 5.3.3. ISO/IEC-mdoc EAAP Response profile (ISO/IEC-mdoc EAAP-válaszprofil)

— Ez a pont meghatározza a DeviceResponse üzenettípusra vonatkozó követelményeket, amelyek mindkét típusú átviteli mechanizmus (API-n keresztüli és nem API-n keresztüli) esetében azonosak

— *1. MEGJEGYZÉS*: Az ISO/IEC 18013-5 [10] szabványon alapuló, nem API-n keresztüli mechanizmus alkalmazása esetén az EAAP-válasz pontosan az e pontban leírt DeviceResponse profilnak felel meg. Az ISO/IEC 18013-7 [16] szabvány C. mellékletén alapuló, API-n keresztüli mechanizmus alkalmazása esetén a DeviceRequest adatokat a [16] szabvány C. mellékletében meghatározottak szerint kell beágyazni

— ISO/IEC 18013-5-RESP-02: A személyazonosító adatok és az elektronikus attribútumtanúsítványok szolgáltatója az általa kibocsátott személyazonosító adatok, illetve elektronikus attribútumtanúsítványok mobilbiztonsági objektumában nem tüntethet fel adatelemeket a KeyAuthorizations adatstruktúrában, azon adatelemek kivételével, amelyeket az adattárca-igénybevevő az adattárcaegység által a személyazonosító adatok vagy az elektronikus attribútumtanúsítványok privát kulcsának felhasználásával aláírással vagy bélyegzővel ellátandó mdoc kérelemben szereplő tranzakciós adatokban megad

— *2. MEGJEGYZÉS*: Ennek eredményeként az adattárcaegységek nem jeleníthetnek meg az adattárca-igénybevevők számára eszköz által aláírt adatelemeket, kivéve az adattárca-igénybevevő által szolgáltatott aláírási adatokat, például biztonságos felhasználóhitelesítés céljából

— *3. MEGJEGYZÉS*: Az ISO/IEC 18013-5:2021 szabvány nem határozza meg, hogy az adattárca-igénybevevők hogyan foglalhatnak tranzakciós adatokat az mdoc kérelembe. A tranzakciós adatok mdoc kérelembe való belefoglalása technikai specifikációk hozzáadásával történik

— ISO/IEC 18013-5-RESP-03: A személyazonosítóadat-szolgáltatók nem engedélyezhetik, hogy a személyazonosító adatok privát kulcsa aláírással lássa el az adattárca-igénybevevő által az mdoc kérelemben megadott tranzakciós adatokban szereplő adatelemeket

11. 5.4. Requirements for API mediated mechanism (Az API-n keresztüli mechanizmusokra vonatkozó követelmények)

5.4.1. ISO/IEC 18013-7-related requirements (ISO/IEC 18013-7-hez kapcsolódó követelmények)

Ez a pont meghatározza a [16] szabvány C. mellékletében lefektetett követelményekhez kapcsolódó, az API-n keresztüli átviteli mechanizmusra vonatkozó követelményeket.

— ISO/IEC 18013-7-API-01: Az API-alapú megjelenítéseket támogató profilnak meg kell felelnie az ISO/IEC 18013-7 [16] szabvány C. mellékletében foglalt követelményeknek, az e dokumentum 5.3. és 5.4. pontjában leírt részletesebb profiloknak megfelelően

— ISO/IEC 18013-7-API-02: A [16] szabvány C. mellékletében meghatározott valamennyi kötelező követelményt alkalmazni kell, az e dokumentum 5.3. és 5.4. pontjában leírt részletesebb profiloknak megfelelően

— ISO/IEC 18013-7-API-03: A [16] szabvány C. mellékletében meghatározott valamennyi opcionális követelmény opcionális marad, kivéve, ha e dokumentum másként rendelkezik

12. 5.4.2. Additional requirements (További követelmények)

— Ez a pont további követelményeket határoz meg az API-n keresztüli átviteli mechanizmusra vonatkozóan

— ISO/IEC 18013-ADD-API-01: Az európai digitális személyiadat-tárcának alapértelmezés szerint közölnie kell az összes tárolt elektronikus attribútumtanúsítvány típusát a [16] szabvány C. melléklete szerint működő közvetítő API-val, de az attribútumokat és azok értékeit nem fedheti fel az elektronikus attribútum-tanúsítványokban

— *1. MEGJEGYZÉS*: Az attribútumértékekre vonatkozó korlátozás akkor is alkalmazandó, ha ezek felfedése javítaná az operációs rendszer által az európai digitális személyiadat-tárcának nyújtott szolgáltatásokat, például a közvetítő API kapcsán segítené a tanúsítványok kiválasztását

— Egyes, az operációs rendszerekkel és a böngészőkkel kapcsolatos megfontolások kívül esnek az alkalmazók hatáskörén; ezeket az alábbi 2–4. megjegyzésben foglaltak szerint lehet figyelembe venni:

— *2. MEGJEGYZÉS*: Az igénybe vevő féltől származó, a [16] szabvány C. mellékletét támogató megjelenítési kérést a böngésző és/vagy az operációs rendszer a rendelkezésre álló EAA-k keresése, a felhasználóra irányuló csalások megelőzése vagy hibaelhárítás céljából dolgozhatja fel

— *3. MEGJEGYZÉS*: A [16] szabvány C. mellékletét támogató, az igénybe vevő fél által benyújtott megjelenítési kérést a böngésző és/vagy az operációs rendszer felhasználóbiztonsági célokból dolgozhatja fel

— 4. *MEGJEGYZÉS*: A [16] szabvány C. mellékletét támogató, az igénybe vevő fél által benyújtott megjelenítési kérést a böngésző és/vagy az operációs rendszer nem dolgozhatja fel piacelemzési célra (másodlagos célként sem), illetve a böngésző és/vagy az operációs rendszer belső céljaira

— ISO/IEC 18013-ADD-API-02: Amennyiben egy európai digitális személyiadat-tárca a felhasználó kérésére törli a [16] szabvány C. melléklete szerint működő közvetítő API-val korábban közölt PID vagy EAA adatait, az európai digitális személyiadat-tárcának közölnie kell a közvetítő API-val, hogy az érintett PID vagy EAA már nincs tárolva rajta

— ISO/IEC 18013-ADD-API-03: Ha a felhasználó eltávolítja az európai digitális személyiadat-tárcáját, az európai digitális személyiadat-tárcának közölnie kell a [16] szabvány C. melléklete szerint működő közvetítő API-val, hogy már nem tárol korábban közzétett PID vagy EAA adatokat

— ISO/IEC 18013-ADD-API-04: Az európai digitális személyiadat-tárcának lehetővé kell tennie egy olyan globális felhasználói beállítást, amely letiltja a tárolt EAA adatok felfedését az ISO/IEC 18013-ADD-API-01 szabvány szerint működő közvetítő API-n keresztül. Ha ez a beállítás ki van kapcsolva, az európai digitális személyiadat-tárca nem kapcsolódhat és nem válaszolhat az API-n keresztül érkező megjelenítési vagy kibocsátási kérésekre

— ISO/IEC 18013-ADD-API-05: Az európai digitális személyiadat-tárcák az eszközök közötti adatátvitel során a közvetítő API használatával, biztonságos, közvetlen és felhasználói közvetítésű helyi kommunikációs csatornát, például rövid hatótávolságú, vezeték nélküli kommunikációs technológiát használva ellenőrzik, hogy az interakciót végző eszköz az európai digitális személyiadat-tárca közvetlen fizikai közelében van-e

— *MEGJEGYZÉS*: A CTAP 2.3. verziója lehetővé teszi a BLE specifikáció használatát a fizikai közelség ellenőrzésére, és ha mindkét eszköz ezt alkalmazza, az adatok kis hatótávolságú átviteli technológiákkal történő továbbítását is lehetővé teszi az eszközök között. Az alapul szolgáló operációs rendszereknek, böngészőknek, közvetítő API-knak vagy bármely más, az európai digitális személyiadat-tárca által nem befolyásolható technikai rétegnek a CTAP hibrid alagút szolgáltatásainak használatával szemben előnyben kell részesítenie, hogy mind a fizikai közelség ellenőrzése, mind a két eszköz közötti adattovábbítás a CTAP 2.3 által biztosított helyi kommunikációs csatornán történjen

13. 6.2. Requirements on EUDI Wallet and RP support (Az európai digitális személyiadat-tárca és az RP általi támogatásra vonatkozó követelmények)

— OIDFVP-HAIP-SUPPORT-02: Az európai digitális személyiadat-tárcának meg kell felelnie az e melléklet 6.5. pontjában meghatározott követelményeknek

— OIDFVP-HAIP-SUPPORT-03: Az európai digitális személyiadat-tárca nem támogathatja a 6.4. pontban meghatározott, az eszközök közötti megjelenítési folyamatokra vonatkozó, redirects-alapú mechanizmust

— 3. MEGJEGYZÉS: E mechanizmus használata – többek között munkamenet-rögzítéses – támadások veszélyével járhat. Az ilyen támadások kockázatának csökkentése az igénybe vevő felek feladata. E mechanizmus alkalmazása nem eredményezhet meg nem felelést

— OIDFVP-HAIP-SUPPORT-05: Az igénybe vevő félnek meg kell felelnie az e melléklet 6.5. pontjában meghatározott követelményeknek

— 5. *MEGJEGYZÉS*: érvénytelen

14. 6.3.1. General requirements (Általános követelmények)

— OIDFVP-HAIP-GEN-01: A HAIP [11] 5., 5.3., 7. és 8. pontjában meghatározott valamennyi kötelező követelményt alkalmazni kell

— 1. *MEGJEGYZÉS*: A „HAIP [11] 5. szakasz” csak a közvetlenül az 5. szakasz címe alatti követelményekre vonatkozik. Nem foglalja magában az 5.1., 5.2. és 5.3. szakaszt

— OIDFVP-HAIP-GEN-03: Ha e melléklet módosítja az OpenID4VC-HAIP [11] valamelyik követelményét, az e mellékletben meghatározott módosított követelmény az irányadó

— 2. *MEGJEGYZÉS*: Ez lehetővé teheti például az OpenID4VC-HAIP [11] egy opcionális követelményének kötelezővé tételét, vagy a kötelező követelmények kiterjesztését

— OIDFVP-HAIP-GEN-04: Amennyiben a kért tanúsítvány formátuma megfelel a [10] szabványnak, az igénybe vevő félnek és az európai digitális személyiadat-tárcáknak meg kell felelniük a [11] szabvány 6. szakaszában szereplő „ISO-mdocs” profilnak

— 3. *MEGJEGYZÉS*: Az egyértelműség érdekében: a HAIP-ban az „ISO-mdocs profil” azt jelenti, hogy az igénybe vevő feleknek és az európai digitális személyiadat-tárcáknak meg kell felelniük a [7] szabvány B.2. mellékletben foglalt alkalmazandó követelményeknek

— OIDFVP-HAIP-GEN-05: Ha a kért tanúsítvány formátuma megfelel a [2] szabványnak, az igénybe vevő feleknek és az európai digitális személyiadat-tárcáknak meg kell felelniük a [11] szabvány 6. szakaszában szereplő „IETF SD-JWT VCs” profilnak

— 4. *MEGJEGYZÉS*: Az egyértelműség érdekében: az „IETF SD-JWT VCs profil” azt jelenti, hogy az igénybe vevő feleknek és az európai digitális személyiadat-tárcáknak meg kell felelniük a [7] szabvány B.3. mellékletében, valamint a [11] szabvány 6.1. szakaszában foglalt követelményeknek

15. 6.3.2.1. General requirements (Általános követelmények)

— OIDFVP-HAIP-COMMON-REQ-01: érvénytelen

16. 6.3.2.2. Requirements for the Request Object (A kérésobjektumra vonatkozó követelmények)

— OIDFVP-HAIP-COMMON-REQ-RO-02: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-03: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-04: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-05: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-06: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-07: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-08: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-09: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-10: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-11: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-12: érvénytelen

— 2. megjegyzés: érvénytelen

— OIDFVP-HAIP-COMMON-REQ-RO-13: A verifier_info paraméter egyik elemének tartalmaznia kell a nyilvántartási tanúsítványt

— OIDFVP-HAIP-COMMON-REQ-RO-23: Az OpenID4VP 5.9.3. szakaszában említett, az x509_hash ügyfélazonosító előtaggal való használatra szolgáló végfelhasználói tanúsítvány az ETSI TS 119 475 [14] szabványban meghatározott RP hozzáférési tanúsítvány

17. 6.3.3. Authorization Response (EAAP response) profile (Engedélyezési válasz [EAAP-válasz] profil)

— OIDFVP-HAIP-COMMON-RESP-01: érvénytelen

18. 6.4.1. General requirements (Általános követelmények)

— OIDFVP-HAIP-REDIRECTS-04: érvénytelen

— MEGJEGYZÉS: érvénytelen

19. 6.5.2 Additional requirements (További követelmények)

— OIDFVP-HAIP-ADD-API-01: Az európai digitális személyiadat-tárcának alapértelmezés szerint fel kell fednie az összes tárolt EAA típus jelenlétét a [11] szabvány 5.2. pontja szerint működő közvetítő API számára, de nem fedheti fel az EAA adatokban lévő attribútumokat és azok értékeit

— OIDFVP-HAIP-ADD-API-04: Ha az európai digitális személyiadat-tárca támogat egy, az OIDFVP-HAIP-ADD-API-01 szerint működő közvetítő API-t, akkor lehetővé kell tennie egy olyan globális felhasználói beállítást, amely letiltja a tárolt EAA adatok közvetítő API-n keresztül történő felfedését. Ha ez a beállítás a felfedés letiltására van beállítva, az európai digitális személyiadat-tárcának lehetővé kell tennie a felhasználó számára, hogy kiválassza a közvetítő API részére felfedhető egyedi tanúsítványokat

— OIDFVP-HAIP-ADD-API-05: Az európai digitális személyiadat-tárcák az eszközök közötti adatátvitel során a közvetítő API használatával, biztonságos, közvetlen és felhasználói közvetítésű helyi kommunikációs csatornát, például rövid hatótávolságú, vezeték nélküli kommunikációs technológiát használva ellenőrzik, hogy az interakciót végző eszköz az európai digitális személyiadat-tárca közvetlen fizikai közelében van-e

— *5. MEGJEGYZÉS*: A CTAP 2.3. verziója lehetővé teszi a BLE specifikáció használatát a fizikai közelség ellenőrzésére, és ha mindkét eszköz ezt alkalmazza, az adatok kis hatótávolságú átviteli technológiákkal történő továbbítását is lehetővé teszi az eszközök között. Az alapul szolgáló operációs rendszereknek, böngészőknek, közvetítő API-knak vagy bármely más, az európai digitális személyiadat-tárca által nem befolyásolható technikai rétegnek a CTAP hibrid alagút szolgáltatásainak használatával szemben előnyben kell részesítenie, hogy mind a fizikai közelség ellenőrzése, mind a két eszköz közötti adattovábbítás a CTAP 2.3 által biztosított helyi kommunikációs csatornán történjen

20. 6.5.3. Specific requirements when requesting ISO/IEC 18013-5 EAAP (ISO/IEC 18013-5 EAAP kérése esetén alkalmazandó egyedi követelmények)

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Az e dokumentumban meghatározott, az ISO/IEC 18013-5 szabvány szerinti eszközkérés- és eszközválasz-struktúrákra alkalmazandó valamennyi követelmény akkor is alkalmazandó, ha az európai digitális személyiadat-tárca a [16] szabvány C.1. pontja szerinti, API-n keresztül továbbított mechanizmus révén ISO/IEC mdoc megjelenítésére irányuló kérést kap.”