►B

A BIZOTTSÁG (EU) 2021/1073 VÉGREHAJTÁSI HATÁROZATA

(2021. június 28.)

az (EU) 2021/953 európai parlamenti és tanácsi rendelettel létrehozott uniós digitális Covid-igazolvány bizalmi keretrendszere technikai előírásainak és végrehajtása szabályainak meghatározásáról

(EGT-vonatkozású szöveg)

(HL L 230., 2021.6.30., 32. o.)

Módosította:

		Hivatalos Lap		
		Szám	Oldal	Dátum
►M1	A Bizottság (EU) 2021/2014 végrehajtási határozata (2021. november 17.)	L 410	180	2021.11.18.
►M2	A Bizottság (EU) 2021/2301 végrehajtási határozata (2021. december 21.)	L 458	536	2021.12.22.
►M3	A Bizottság (EU) 2022/483 végrehajtási határozata (2022. március 21.)	L 98	84	2022.3.25.
►M4	A Bizottság (EU) 2022/1516 végrehajtási határozata (2022. szeptember 8.)	L 235	61	2022.9.12.

▼B

A BIZOTTSÁG (EU) 2021/1073 VÉGREHAJTÁSI HATÁROZATA

(2021. június 28.)

az (EU) 2021/953 európai parlamenti és tanácsi rendelettel létrehozott uniós digitális Covid-igazolvány bizalmi keretrendszere technikai előírásainak és végrehajtása szabályainak meghatározásáról

(EGT-vonatkozású szöveg)

1. cikk

Az uniós digitális Covid-igazolványra vonatkozó műszaki előírásokat, amelyek meghatározzák az általános adatszerkezetet, a kódolási mechanizmusokat és a géppel olvasható optikai formátumban történő továbbítási kódolási mechanizmust, az I. melléklet tartalmazza.

2. cikk

Az (EU) 2021/953 rendelet 3. cikkének (1) bekezdésében említett igazolványok kitöltésére vonatkozó szabályokat e határozat II. melléklete tartalmazza.

3. cikk

Az egyedi igazolványazonosító közös szerkezetét meghatározó követelményeket a III. melléklet tartalmazza.

▼M1

4. cikk

Az uniós digitális Covid-igazolványnak a bizalmi keretrendszer interoperabilitási szempontjait támogató átjárójához kapcsolódóan a nyilvános kulcsok tanúsítványaira alkalmazandó irányítási szabályokat a IV. melléklet tartalmazza.

5. cikk

Az (EU) 2021/953 rendelet 3. cikkének (1) bekezdésében említett igazolványokban feltüntetendő adatok közös, összehangolt – a JavaScript Objektum Jelölés (JSON) sémát használó – adatszerkezetét e határozat V. melléklete tartalmazza.

▼M3

5a. cikk

A visszavont igazolványok jegyzékeinek cseréje

(1) Az uniós digitális Covid-igazolvány bizalmi keretrendszerének lehetővé kell tennie a visszavont igazolványok jegyzékeinek cseréjét az uniós digitális Covid-igazolvány központi átjáróján (a továbbiakban: az átjáró) keresztül, az I. mellékletben foglalt műszaki előírásokkal összhangban.

(2) Amennyiben a tagállamok uniós digitális Covid-igazolványokat vonnak vissza, a visszavont igazolványok jegyzékeit benyújthatják az átjárónak.

▼M3

(3) Amennyiben a tagállamok benyújtják a visszavont igazolványok jegyzékeit, a kiállító hatóságok jegyzéket vezetnek a visszavont igazolványokról.

(4) Amennyiben az átjárón keresztül személyes adatok cseréjére kerül sor, az adatkezelésnek a visszavonással kapcsolatos információk cseréjének támogatására kell korlátozódnia. Az ilyen személyes adatok kizárólag az (EU) 2021/953 rendelet hatálya alá tartozó uniós digitális Covid-igazolványok visszavont státuszának ellenőrzése céljából használhatók fel.

(5) Az átjárónak benyújtott információk az I. mellékletben foglalt műszaki előírásoknak megfelelően a következő adatokat tartalmazzák:

a) a visszavont igazolványok álnevesített egyedi igazolványazonosítói,

b) a visszavont igazolványok jegyzékének lejárati időpontja;

(6) Amennyiben a kiállító hatóság az (EU) 2021/953 rendelet vagy az (EU) 2021/954 rendelet alapján általa kiállított uniós digitális Covid-igazolványokat von vissza, és releváns információkat kíván cserélni az átjárón keresztül, az (5) bekezdésben említett információkat a visszavont igazolványok jegyzékei formájában, az I. mellékletben foglalt műszaki előírásoknak megfelelően biztonságos formátumban továbbítja az átjárónak.

(7) A kiállító hatóságok lehetőség szerint megoldást kínálnak arra, hogy a visszavont igazolványok birtokosait a visszavonás időpontjában tájékoztassák igazolványuk visszavonási státuszáról és a visszavonás okáról.

(8) Az átjáró összegyűjti a visszavont igazolványok beérkezett jegyzékeit, és eszközöket biztosít a jegyzékek tagállamok közötti terjesztéséhez. Automatikusan törli a jegyzékeket az egyes benyújtott jegyzékekre vonatkozóan a benyújtó hatóság által megadott lejárati időpontoknak megfelelően.

(9) Az átjárón keresztül személyes adatokat kezelő kijelölt nemzeti hatóságok vagy hivatalos szervek a kezelt adatok közös adatkezelői. A közös adatkezelők felelősségi köreit a VI. mellékletnek megfelelően kell kiosztani.

(10) A Bizottság az átjárón keresztül feldolgozott személyes adatok feldolgozója. A Bizottság a tagállamok nevében adatfeldolgozóként biztosítja a személyes adatok továbbításának és tárolásának biztonságát az átjárón belül, és eleget tesz az adatfeldolgozó VII. mellékletben meghatározott kötelezettségeinek.

(11) A Bizottság és a közös adatkezelők rendszeresen tesztelik, felmérik és értékelik az átjárón belül a személyes adatok biztonságos kezelését biztosító technikai és szervezési intézkedések hatékonyságát.

▼M3

5b. cikk

A visszavont igazolványok jegyzékeinek harmadik országok általi benyújtása

Azok a Covid19-igazolványokat kiállító harmadik országok, amelyek tekintetében a Bizottság az (EU) 2021/953 rendelet 3. cikkének (10) bekezdése vagy 8. cikkének (2) bekezdése alapján végrehajtási jogi aktust fogadott el, benyújthatják az ilyen végrehajtási jogi aktus hatálya alá tartozó visszavont Covid19-igazolványok jegyzékét, amelyeket a Bizottság az 5a. cikkben említett átjárón a közös adatkezelők nevében az I. mellékletben meghatározott technikai előírásoknak megfelelően kezel.

5c. cikk

A személyes adatok kezelésének irányítása az uniós digitális Covid-igazolvány központi átjáróján

(1) A közös adatkezelők döntéshozatali eljárását az (EU) 2021/953 rendelet 14. cikkében említett bizottság keretében létrehozott munkacsoport irányítja.

(2) Az átjárón keresztül személyes adatokat kezelő kijelölt nemzeti hatóságok vagy hivatalos szervek közös adatkezelőként kijelölik az említett csoport képviselőit.

▼M1

6. cikk

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetésének napján lép hatályba.

▼B

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetésének napján lép hatályba.

▼B

I. MELLÉKLET

FORMÁTUM ÉS BIZALMI KEZELÉS

Általános adatszerkezet, kódolási mechanizmusok és a géppel olvasható optikai formátumban (a továbbiakban: QR) történő továbbítási kódolási mechanizmus

1. **Bevezetés**

A jelen mellékletben meghatározott technikai előírások tartalmazzák az uniós digitális Covid-igazolvány (a továbbiakban: DCC) általános adatszerkezetét és kódolási mechanizmusait. Emellett egy olyan, géppel olvasható optikai továbbítási kódolási mechanizmust (QR) is meghatároznak, amely megjeleníthető egy mobil eszköz képernyőjén, vagy papírra kinyomtatható. Az elektronikus egészségügyi igazolvány ezen előírásokban szereplő konténerformátumai általánosak, de ebben az összefüggésben a DCC-t jelenítik meg.

2. **Terminológia**

E melléklet alkalmazásában a „kibocsátók” azok a szervezetek, amelyek ezeket az előírásokat használják az egészségügyi igazolványok kiállításához, az „ellenőrzők” pedig olyan szervezetek, amelyek az egészségügyi állapot igazolásaként egészségügyi igazolványokat fogadnak el. A „résztvevők” a kibocsátók és az ellenőrzők. Az e mellékletben meghatározott egyes szempontokat – mint például a névtartomány kezelését és a kriptográfiai kulcsok kiosztását – össze kell hangolni a résztvevők között. Abból kell kiindulni, hogy egy fél – a továbbiakban: titkárság – látja el ezeket a feladatokat.

3. **Az elektronikus egészségügyi igazolvány konténerformátuma**

Az elektronikus egészségügyi igazolvány konténerformátumának (HCERT) célja, hogy egy egységes és szabványosított eszközt biztosítson a különböző kibocsátók (a továbbiakban: kibocsátók) által kiállított egészségügyi igazolványokhoz. Ezen előírások célja az, hogy összehangolják az említett egészségügyi igazolványok megjelenítésének, kódolásának és aláírásának módját az interoperabilitás megkönnyítése érdekében.

A bármely kibocsátó által kibocsátott DCC olvasása és értelmezése szükségessé teszi a közös adatstruktúrát és a hasznos adatok egyes adatmezőinek szignifikanciájára vonatkozó megállapodást. Az ilyen interoperabilitás előmozdítása érdekében egy közös összehangolt adatstruktúra kerül meghatározásra a „JSON” séma használatával, amely a DCC keretét alkotja.

3.1. *A hasznos adatok szerkezete*

A hasznos adatok szerkezete és kódolása CBOR-ként történik, COSE digitális aláírással. Ennek közismert neve „CBOR Web Token” (CWT), és az RFC 8392 előírás ([1]) határozza meg. A következő szakaszokban meghatározott hasznos adatokat egy hcert kérésként továbbítják.

A hasznos adatok sértetlenségét és eredetének hitelességét az ellenőrzőnek kell ellenőriznie. E mechanizmus biztosítása érdekében a kibocsátónak a COSE-előírásban (RFC 8152 ([2])) meghatározott aszimmetrikus elektronikus aláírási rendszer használatával kell aláírnia a CWT-t.

3.2. *CWT kérések*

3.2.1. A CWT szerkezetének áttekintése

Védett fejléc

([1]) rfc8392 (ietf.org).
([2]) rfc8152 (ietf.org).

▼B

— Aláírás-algoritmus (alg, 1. címke)

— Kulcsazonosító (kid, 4. címke)

Hasznos adatok

— Kibocsátó (iss, 1. kulcskérés, opcionális, a kibocsátó ISO 3166-1 szerinti alpha-2-es kódja)

— Kibocsátás időpontja (iat, 6. kulcskérés)

— Lejárat időpontja (exp, 4. kulcskérés)

— Egészségügyi igazolvány (hcert, –260 kulcskérés)

— Uniós digitális Covid-igazolvány v1 (eu_DCC_v1, 1. kulcskérés)

Aláírás

3.2.2. Aláírás algoritmus

Az Aláírás algoritmus (alg) paraméter jelzi, hogy milyen algoritmust használtak az aláírás létrehozatalához. Ennek meg kell felelnie az alábbi bekezdésekben összefoglalt jelenlegi SOG-IS iránymutatásoknak, vagy meg kell haladnia azokat.

Egy elsődleges és egy másodlagos algoritmust kell meghatározni. A másodlagos algoritmust csak akkor szabad használni, ha az elsődleges algoritmus nem elfogadható a kibocsátóra vonatkozó szabályok és előírások szerint.

A rendszer biztonságának biztosítása érdekében minden végrehajtásnak tartalmaznia kell a másodlagos algoritmust. Ezért mind az elsődleges, mind a másodlagos algoritmust végre kell hajtani.

Az elsődleges és másodlagos algoritmusok SOG-IS-értékei a következők:

— Elsődleges algoritmus: Az elsődleges algoritmus az ISO/IEC 14888-3:2006 szabvány 2.3. szakaszában meghatározott Elliptikus görbéken alapuló digitális aláírási algoritmus (ECDSA), a FIPS PUB 186-4 D. függelékében (D.1.2.3) meghatározott P-256 paramétereket az ISO/IEC 10118-3:2004 szabvány 4. funkciójában meghatározott SHA-256 hash algoritmussal kombináltan használva.

Ez az ES256 COSE algoritmus paraméternek felel meg.

— Másodlagos algoritmus: A másodlagos algoritmus az (RFC 8230 ([1])) meghatározása szerinti RSASSA-PSS, 2048 bites modulussal, az ISO/IEC 10118-3:2004 szabvány 4. funkciójában meghatározott SHA-256 hash algoritmussal kombinálva.

Ez a COSE algoritmus következő paraméterének felel meg: PS256.

3.2.3. Kulcsazonosító

A Kulcsazonosító (kid) kérés azt a dokumentum-aláíró tanúsítványt (DSC) jelöli, amely tartalmazza az ellenőrző által a digitális aláírás helyességének ellenőrzéséhez használandó nyilvános kulcsot. A nyilvánoskulcs-tanúsítványok irányítását, beleértve a DSC-kre vonatkozó követelményeket is, a IV. melléklet ismerteti.

([1]) rfc8230 (ietf.org).

▼B

A Kulcsazonosító (kid) kérést az ellenőrzők használják a megfelelő nyilvános kulcs kiválasztására a Kibocsátó (iss) kérésben megjelölt kibocsátóra vonatkozó kulcsok listájából. Egy kibocsátó egyidejűleg több kulcsot is használhat adminisztratív okokból és a kulcscserék végrehajtásakor. A Kulcsazonosító a biztonság szempontjából nem kritikus mező. Ezért, ha szükséges, nem védett fejlécben is elhelyezhető. Az ellenőrzők mindkét lehetőséget kötelesek elfogadni. Ha mindkét megoldást alkalmazzák, akkor a védett fejlécben található Kulcsazonosítót kell használni.

Az azonosító (méretkorlát miatti) lerövidítése következtében kevés, de nem nulla esély van arra, hogy az ellenőrző által elfogadott DSC-k teljes listájában lehetnek kettős kid-eket tartalmazó DSC-k. Ezért az ellenőrzőnek az adott kid-del rendelkező valamennyi DSC-t ellenőriznie kell.

3.2.4. Kibocsátó

A Kibocsátó (iss) kérése egy olyan karakterláncérték, amely opcionálisan rendelkezhet az egészségügyi igazolványt kiállító szervezet ISO 3166-1 szerinti alpha-2-es országkódjával. Ezt a kérést az ellenőrző felhasználhatja annak azonosítására, hogy az ellenőrzéshez melyik DSC-csoportot kell használni. Ennek a kérésnek az azonosítására az 1. Kulcs kérés szolgál.

3.2.5. Lejárati idő

A Lejárati idő (exp) kérésnek időbélyegzővel kell rendelkeznie az egész számot tartalmazó NumericDate formátumban (az RFC 8392 ([1]) szabvány 2. szakaszában meghatározottak szerint), amely jelzi, hogy a hasznos adatokra vonatkozó adott aláírás mennyi ideig tekintendő érvényesnek, és ezt követően az ellenőrzőnek lejárat miatt el kell utasítania a hasznos adatokat. A lejárati paraméter célja az egészségügyi igazolvány érvényességi idejének korlátozása. Ennek a kérésnek az azonosítására a 4. Kulcs kérés szolgál.

A lejárati idő nem haladhatja meg a DSC érvényességi idejét.

3.2.6. Kibocsátás időpontja

A Kibocsátás időpontja (iat) kérésnek egész számot tartalmazó NumericDate formátumú időbélyegzővel kell rendelkeznie (az RFC 8392 ([2]), szabvány 2. szakaszában meghatározottak szerint), feltüntetve az egészségügyi igazolvány létrehozásának időpontját.

A Kibocsátás időpontja mező nem lehet korábbi, mint a DSC érvényességi időtartama.

Az ellenőrzők további szabályokat alkalmazhatnak azzal a céllal, hogy korlátozzák az egészségügyi igazolvány érvényességét a kibocsátás időpontja alapján. Ennek a kérésnek az azonosítására a 6. Kulcs kérés szolgál.

3.2.7. Egészségügyi igazolvány kérés

Az Egészségügyi igazolvány (hcert) kérés egy JSON (RFC 7159 ([3])) objektum, amely tartalmazza az egészségügyi állapotra vonatkozó információt. Ugyanazon kérés alapján több különböző típusú egészségügyi igazolvány is létezhet, amelyek közül a DCC egy.

A JSON tisztán csak séma célokat szolgál. A reprezentációs formátum az RFC 7049 ([4]) szabványban meghatározott CBOR. Az alkalmazásfejlesztők valójában sohasem dekódolják vagy kódolják a JSON-formátumot, hanem a memóriában található szerkezetet használhatják.

([1]) rfc8392 (ietf.org).
([2]) rfc8392 (ietf.org).
([3]) rfc7159 (ietf.org).
([4]) rfc7049 (ietf.org).

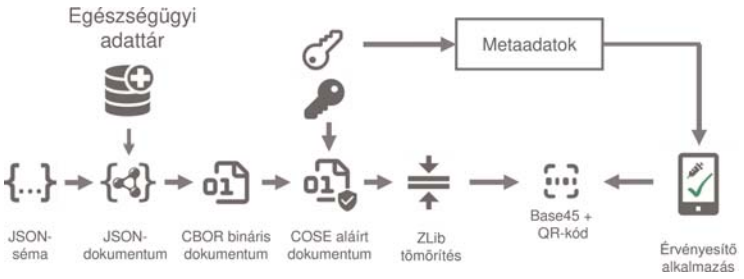
▼B

Ennek a kérésnek az azonosítására a –260 Kulcs kérés szolgál.

A JSON objektumban lévő karakterláncokat az Unicode szabványban meghatározott kanonikus kompozíciós normalizálási forma (NFC) szerint normalizálni kell. A dekódolási alkalmazásoknak azonban megengedőnek és megbízhatónak kell lenniük e tekintetben, és határozottan ösztönözni kell bármely észszerű típus-átalakítás elfogadását. Ha a dekódolás során vagy az azt követő összehasonlítási funkciókban nem normalizált adatokat találnak, a végrehajtásnak úgy kell történnie, mintha a bevitelt normalizálnák az NFC-re.

4. **A DCC hasznos adatainak szerializációja és létrehozása**

A következő eljárást kell szerializációs mintaként használni:



A folyamat az adatoknak például egy Egészségügyi adattárból (vagy valamely külső adatforrásból) történő kinyerésével kezdődik, amely a kinyert adatokat a meghatározott DCC sémák szerint strukturálja. Ebben a folyamatban a meghatározott adatformátumra való átváltásra és az emberi olvashatóság érdekében történő átalakításra a CBOR-ra történő szerializáció megkezdése előtt sor kerülhet. A kérések rövidítéseit minden esetben a szerializáció előtt és a deszerializációt követően hozzá kell rendelni a megjelenített nevekhez.

Az (EU) 2021/953 rendelet ([1]) alapján kiállított igazolványok nem tartalmazhatnak opcionális nemzeti adattartalmat. Az adattartalom a 2021/953 rendelet mellékletében meghatározott minimális adatkészletben meghatározott adatelemekre korlátozódik.

5. **Továbbítási kódolások**

5.1. *Nyers*

Tetszőleges adatinterfészek esetében a HCERT konténere és hasznos adatai az adott állapotban továbbíthatók, az alapul szolgáló bármely 8 bites biztonságos, megbízható adattovábbítás felhasználásával. Ezek az interfészek magukban foglalhatják a kis hatótávolságú kommunikációt (NFC), a Bluetooth-t vagy az alkalmazási rétegbeli protokollon keresztüli továbbítást, például a HCERT továbbítását a Kibocsátótól a birtokos mobil eszközére.

Ha a HCERT-nek a Kibocsátótól a birtokoshoz történő továbbítása kizárólag prezentáló interfészen alapul (például SMS, e-mail), a nyers továbbítási kódolás nyilvánvalóan nem alkalmazható.

([1]) Az Európai Parlament és a Tanács (EU) 2021/953 rendelete (2021. június 14.) a Covid19-világjárvány idején a szabad mozgás megkönnyítése érdekében az interoperábilis, Covid19-oltásra, tesztre és gyógyultságra vonatkozó igazolványok (uniós digitális Covid-igazolvány) kiállításának, ellenőrzésének és elfogadásának keretéről (HL L 211., 2021.6.15., 1. o.).

▼B

5.2. *Vonalkód*

5.2.1. Hasznos adat (CWT) tömörítés

A HCERT méretének csökkentése, valamint leolvasási folyamata sebességének és megbízhatóságának javítása érdekében a CWT-t ZLIB-bel (RFC 1950 ([1])) és az RFC 1951 ([2]) szabványban meghatározott Deflate tömörítési mechanizmussal kell tömöríteni.

5.2.2. QR 2D Vonalkód

Az ASCII hasznos adatokon való működésre tervezett, már nem gyártott berendezések jobb kezelése érdekében a tömörített CWT-t a Base45 alkalmazásával ASCII-ként kell kódolni, mielőtt 2D vonalkódba kódolnák.

A 2D vonalkód generálásához az ISO/IEC 18004:2015 szabványban meghatározott QR-formátumot kell használni. Javasolt egy „Q” (körülbelül 25 %) hibajavítási ráta használata. A Base45 használata miatt a QR-kódnak alfanumerikus kódolást kell használnia (2. mód, a 0010 szimbólumokkal jelölve).

Annak érdekében, hogy az ellenőrzők felismerhessék a kódolt adat típusát, és ki tudják választani a megfelelő dekódolási és feldolgozási rendszert, a Base45 kódolt adatokat (ezen előírás szerint) a „HL C 1.:” kontextusazonosító előtag karakterlánccal kell ellátni. Ennek a leírásnak a visszamenőleges kompatibilitást befolyásoló jövőbeli változatai új kontextusazonosítót határoznak majd meg, a „HC”-t követő karaktert pedig az 1–9, A–Z karakterkészletből kell venni. A növekedési sorrend ebben a sorrendben van meghatározva, azaz először 1–9, majd A–Z.

Ajánlott, hogy az optikai kód a prezentáló médiumon 35 mm és 60 mm közötti átlóméretű legyen, hogy megfeleljen a rögzített optikával rendelkező leolvasókhoz, ahol a prezentáló médiumot a leolvasó felületére kell helyezni.

Ha az optikai kódot alacsony felbontású (< 300 dpi) nyomtatók használatával nyomtatják papírra, ügyelni kell arra, hogy a QR-kód minden egyes szimbólumát (pontját) pontosan négyzetesen ábrázolják. A nem arányos méretezés azt eredményezi, hogy a QR egyes sorai vagy oszlopai téglalap alakú szimbólumokkal rendelkeznek, ami sok esetben megnehezíti az olvashatóságot.

6. **Bizalmilista-formátum (CSCA és DSC lista)**

Minden tagállamnak rendelkezésre kell bocsátania egy vagy több országos aláíró hitelesítésszolgáltató (CSCA) listáját, valamint az összes érvényes okmányaláíró tanúsítvány (DSC) jegyzékét, és ezeket a listákat naprakészen kell tartania.

6.1. *Egyszerűsített CSCA/DSC*

Az előírások ezen változatától kezdve a tagállamok nem vélelmezik bármely, a visszavont igazolványok jegyzékére (CRL) vonatkozó információ használatát; vagy azt, hogy a titkos kulcs-használati időszakot a végrehajtók ellenőrzik.

Ehelyett az elsődleges érvényességi mechanizmus az igazolvány feltüntetése az igazolványok jegyzékének legutóbbi változatában.

([1]) rfc1950 (ietf.org).
([2]) rfc1951 (ietf.org).

▼B

6.2. *ICAO eMRTD PKI és bizalmi központok*

A tagállamok használhatnak és benyújthatnak külön CSCA-t, de benyújthatják meglévő eMRTD CSCA tanúsítványaikat és/vagy DSC-iket is; sőt dönthetnek úgy is, hogy ezeket (kereskedelmi) bizalmi központoktól szerzik be. A DSC-t azonban mindig alá kell írnia az adott tagállam által benyújtott CSCA-nak.

7. **Biztonsági megfontolások**

A jelen előírást alkalmazó rendszer kialakításakor a tagállamoknak meghatározott biztonsági szempontokat kell azonosítaniuk, elemezniük és figyelemmel kísérniük.

Minimálisan a következő szempontokat kell figyelembe venni:

7.1. *A HCERT aláírás érvényességi ideje*

A HCERT-ek kibocsátójának az aláírás érvényességi idejét az aláírás lejárati idejének meghatározásával kell korlátoznia. Ez megköveteli, hogy az egészségügyi igazolvány birtokosa rendszeres időközönként megújítsa azt.

Az elfogadható érvényességi időtartamot gyakorlati kötöttségek határozhatják meg. Előfordulhat például, hogy egy utazónak nincs lehetősége arra, hogy egy tengeren túli utazás során megújítsa az egészségügyi igazolványt. Az is előfordulhat azonban, hogy a kibocsátó mérlegeli valamilyen biztonsági kockázat lehetőségét, ami megköveteli, hogy a kibocsátó visszavonja a DSC-t (az e kulcs felhasználásával kibocsátott valamennyi olyan egészségügyi igazolvány érvénytelenítése, amely még az érvényességi időszakon belül van). Egy ilyen esemény következményei korlátozottak lehetnek, ha a kibocsátókulcsokat rendszeresen cserélik, és bizonyos észszerű időközönként előírják valamennyi egészségügyi igazolvány megújítását.

7.2. *Kulcskezelés*

Ez az előírás nagymértékben támaszkodik az erős kriptográfiai mechanizmusokra az adatok sértetlenségének és az adatok eredete hitelesítésének biztosítása érdekében. Ezért szükséges a titkos kulcsokra vonatkozó titoktartás fenntartása.

A kriptográfiai kulcsok titkossága számos különböző módon sérülhet, például:

— a kulcs létrehozásának folyamata hibás lehet, ami gyenge kulcsokat eredményez,

— a kulcsok emberi hiba miatt nyilvánosságra kerülhetnek,

— külső vagy belső elkövetők ellophatják a kulcsokat,

— a kulcsok kriptoanalízis használatával megfejthetők.

Az aláíró algoritmus gyengesége, és így a titkos kulcsok kriptoanalízis útján való sérelme kockázatának csökkentése érdekében, ez az előírás minden résztvevőnek azt ajánlja, hogy az elsődlegestől eltérő paramétereken vagy matematikai problémán alapuló másodlagos tartalék-aláíró algoritmust valósítson meg.

A kibocsátók működési környezetével kapcsolatos említett kockázatok tekintetében a hatékony ellenőrzést biztosító mérséklési intézkedéseket kell végrehajtani, például a biztonsági hardvermodulokban (HSM-ek) található titkos kulcsok létrehozása, tárolása és használata. Az egészségügyi igazolványok aláírásához erősen ösztönzött a HSM-ek használata.

▼B

Függetlenül attól, hogy a kibocsátó a HSM-ek használata mellett dönt-e, ki kell alakítani a kulcsok cseréjének ütemtervét, amelyben a kulcsok cseréjének gyakorisága arányos a kulcsok külső hálózatoknak, egyéb rendszereknek és személyzetnek való kitettségével. A jól megválasztott csere-ütemterv a tévesen kibocsátott egészségügyi igazolványokhoz kapcsolódó kockázatokat is korlátozza, lehetővé téve a kibocsátó számára, hogy az ilyen egészségügyi igazolványokat tételekben visszavonja, szükség esetén a kulcs visszavonásával.

7.3. *A bejövő adatok validálása*

Ezeket az előírásokat oly módon lehet használni, amely magában foglalja adatok érkezését nem megbízható forrásokból olyan rendszerekbe, amelyek a küldetés szempontjából kritikus jelentőségűek lehetnek. Az e támadási vektorral kapcsolatos kockázatok minimalizálása érdekében minden beviteli mezőt adattípus, hossz és tartalom szerint megfelelően validálni kell. A kibocsátó aláírását a HCERT tartalmának feldolgozása előtt is ellenőrizni kell. A kibocsátó aláírásának validálása azonban azt jelenti, hogy először a védett kibocsátó fejlécét kell elemezni, amelybe egy potenciális támadó megpróbálhat a rendszer biztonságát veszélyeztető, gondosan kidolgozott információkat bejuttatni.

8. **Bizalmi kezelés**

A HCERT aláírásának ellenőrzéséhez nyilvános kulcsra van szükség. A tagállamok kötelesek ezeket a nyilvános kulcsokat elérhetővé tenni. Végső soron minden ellenőrzőnek rendelkeznie kell az összes olyan nyilvános kulcs listájával, amelyben kész megbízni (mivel a nyilvános kulcs nem része a HCERT-nek).

A rendszer (csak) két rétegből áll; minden tagállam esetében egy vagy több országos szintű tanúsítvány, amelyek mindegyike aláír egy vagy több, a napi működés során használt dokumentum-aláíró tanúsítványt.

A tagállami tanúsítványokat országos aláíró hitelesítésszolgáltatói (CSCA) tanúsítványnak nevezik, és ezek (jellemzően) saját aláírású tanúsítványok. A tagállamok rendelkezhetnek egynél több ilyennel (például regionális decentralizáció esetén). Ezek a CSCA tanúsítványok szokásosan a HCERT-ek aláírására használt, dokumentumot aláíró tanúsítványokat (DSC-k) írják alá.

A „titkárság” egy funkcionális szerep. Rendszeresen összesíti és közzéteszi a tagállamok DSC-it, miután összevetette azokat a (más módon továbbított és ellenőrzött) CSCA-tanúsítványok listájával.

A DSC-k így kapott listájában meg kell adni azoknak az elfogadható nyilvános kulcsoknak (és a megfelelő KID-eknek) az összesített készletét, amelyeket az ellenőrzők a HCERT-ekre vonatkozó aláírások validálására felhasználhatnak. Az ellenőrzőknek rendszeresen össze kell állítaniuk és frissíteniük kell ezt a listát.

Az ilyen tagállami jegyzékeket a saját nemzeti helyzetüknek megfelelő formátumban át lehet dolgozni. Az ilyen bizalmi lista fájlformátuma változhat, például lehet egy aláírt JWKS (az RFC 7517 ([1]) szabvány 5. szakasza szerinti JWK csoportformátum) vagy bármely más, az adott tagállamban alkalmazott technológiára jellemző formátum.

Az egyszerűség biztosítása érdekében a tagállamok benyújthatják az ICAO eMRTD-rendszereikből származó meglévő CSCA-tanúsítványaikat, vagy – a WHO ajánlásának megfelelően – létrehozhatnak egyet kifejezetten erre az egészségügyi területre vonatkozóan.

([1]) rfc7517 (ietf.org).

▼B

8.1. *A kulcsazonosító (KID)*

A kulcsazonosítót (KID) a DSC-kből származó megbízható nyilvános kulcsok listájának összeállításakor számítják ki, és ez a DSC csonkított (első 8 bájtos) SHA-256 ujjlenyomatából áll, DER (nyers) formátumban kódolva.

Az ellenőrzőknek a DSC alapján nem kell kiszámítaniuk a KID-et, és közvetlenül megfeleltethetik a kiadott egészségügyi igazolványban szereplő kulcsazonosítót a bizalmi listában szereplő KID-del.

8.2. *Eltérések az ICAO eMRTD PKI megbízhatósági modellhez képest*

Bár a rendszer az ICAO eMRTD PKI megbízhatósági modelljének bevált gyakorlatain alapul, a gyorsaság érdekében számos egyszerűsítésre kerül sor:

— Egy tagállam több CSCA tanúsítványt is benyújthat.

— A DSC (kulcshasználat) érvényességi időszaka a CSCA-ét meg nem haladóan bármilyen hosszúságú lehet és hiányozhat is.

— A DSC tartalmazhat az egészségügyi bizonyítványokra specifikus szakpolitikai azonosítókat (kibővített kulcshasználat).

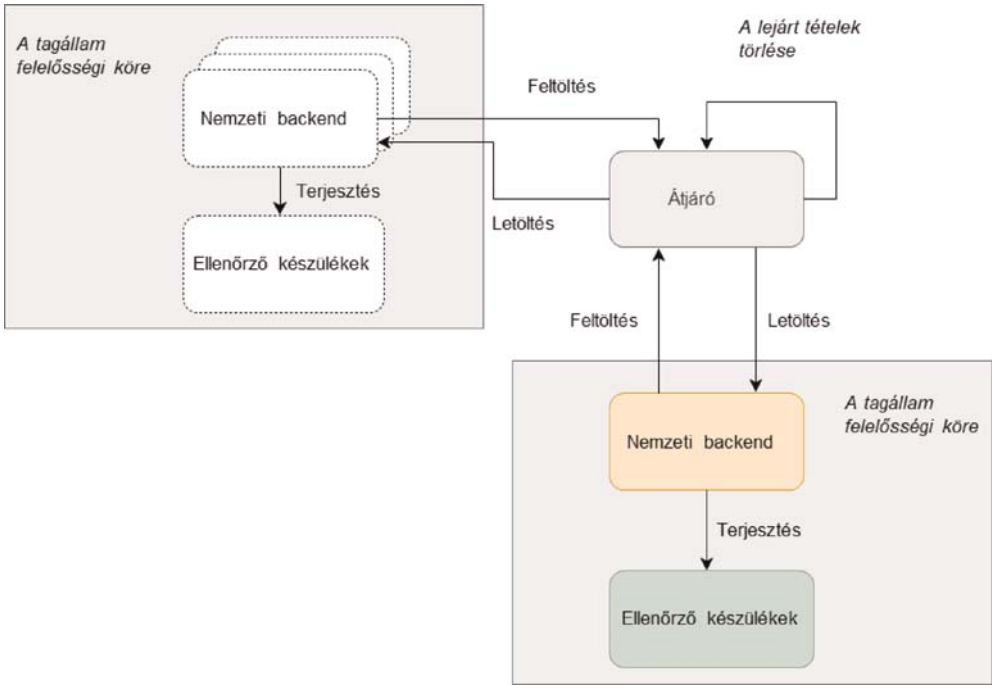
— A tagállamok dönthetnek úgy, hogy soha nem ellenőrzik a közzétett visszavonásokat; ehelyett kizárólag a naponta a titkárságtól kapott vagy az általuk összeállított DSC-listákra támaszkodnak.

▼M3

9. **Megoldás az igazolványok visszavonására**

9.1. *A visszavont DCC-k jegyzékének (DRL) létrehozása*

Az átjáró biztosítja a visszavonási jegyzékek vezetéséhez és kezeléséhez szükséges végpontokat és funkciókat:



▼M3

9.2. *Bizalmi modell*

Minden kapcsolat létesítése a standard DCCG bizalmi modell révén, az NB_{TLS} és NB_{UP} tanúsítványokkal történik. Az integritás biztosítása érdekében valamennyi információ csomagokba rendezve, CMS-üzeneteken keresztül kerül feltöltésre.

9.3. *Tételek egysége*

9.3.1. Tétel

Minden visszavonási jegyzék egy vagy több bejegyzésből áll, és hash-eket és azok metaadatait tartalmazó tételekbe van csomagolva. A tétel megváltoztathatatlan, és egy lejárati időpontot határoz meg, amely jelzi, hogy a tétel mikor törölhető. A tételben szereplő valamennyi elem lejárati időpontjának meg kell egyeznie, azaz a tételeket a lejárati időpont és az aláíró DSC szerint kell csoportosítani. Minden tétel legfeljebb 1 000 bejegyzést tartalmazhat. Ha a visszavonási jegyzék több mint 1 000 bejegyzésből áll, több tételt kell létrehozni. Bármely bejegyzés legfeljebb egy tételben fordulhat elő. A tételt CMS-szerkezetbe kell csomagolni, és a feltöltő ország NB_{UP} tanúsítványával kell aláírni.

9.3.2. Tételindex

Egy tétel létrehozásakor az átjárónak egyedi azonosítót kell a tételhez rendelnie, és azt automatikusan hozzá kell adnia a tételindexhez. A tételindex a módosítás dátuma alapján, növekvő időrendi sorrendbe van rendezve.

9.3.3. Az átjáró viselkedése

Az átjáró változtatás nélkül dolgozza fel a visszavonási tételeket: nem frissítheti, nem távolíthatja el és nem egészítheti ki azokat. A tételeket valamennyi engedélyezett országba továbbítja (lásd a 9.6. szakaszt).

Az átjáró aktívan figyeli a tételek lejárati időpontját, és eltávolítja a lejárt tételeket. A tétel törlése után az átjáró egy „HTTP 410 Gone” válaszüzenetet küld a törölt tétel URL-címére. Ezért a tétel „deleted” (törölt) tételként jelenik meg a tételindexben.

9.4. *Hash típusok*

A visszavonási jegyzék olyan hash-eket tartalmaz, melyek a visszavonás különböző típusait/attribútumait reprezentálhatják. Ezeket a típusokat vagy attribútumokat fel kell tüntetni a visszavonási jegyzékek létrehozásakor. A jelenlegi típusok a következők:

Típus	Attribútum	Hash számítás
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing Country-Code + UCI

Csak a base64 karakterláncként kódolt hash-ek első 128 bitje szerepel a tételekben és kerül felhasználásra a visszavont DCC-k azonosítására ([1]).

([1]) A részletes API-leírásokért, kérjük, vegye figyelembe a 9.5.1.2. szakaszt is.

▼M3

9.4.1. Hash típus: SHA256(DCC Signature)

Ebben az esetben a hash kiszámítása a CWT-ből származó COSE_SIGN1 aláírás bájtjai alapján történik. Az RSA-aláírások esetében a teljes aláírás bemeneti adatként kerül felhasználásra. Az EC–DSA aláírással ellátott tanúsítványok esetében a képlet az r érték a bemeneti adat:

SHA256(r)

[minden új végrehajtás esetében kötelező]

9.4.2. Hash típus: SHA256(UCI)

Ebben az esetben a hash kiszámítása az UTF-8 kódolású UCI karakterlánc alapján történik, és azt bájttömbbé alakítják át.

[elavult ([1]), de a visszamenőleges kompatibilitás érdekében támogatott]

9.4.3. Hash típus: SHA256(Issuing CountryCode+UCI)

Ebben az esetben a CountryCode UTF-8 karakterlánc kódolású UCI-val összefűzött UTF-8 karakterláncként van kódolva. Ezt követően bájttömbbé alakítják át, és a hashfüggvény bemeneti adataként szolgál.

[elavult[2], de a visszamenőleges kompatibilitás érdekében támogatott]

9.5. *API szerkezet*

9.5.1. A visszavonási bejegyzést létrehozó API

9.5.1.1. Cél

Az API a visszavonási listán szereplő bejegyzéseket tételekben állítja elő, melyekhez tételindex is társul.

9.5.1.2. Végpontok

9.5.1.2.1. A tétellista letöltési végpontja

A végpontok egyszerű mintát követnek, és kis csomagolóval metaadatokat rendelkezésre bocsátó tételjegyzéket küldenek vissza. A tételek *dátum* szerint *növekvő (kronológiai)* sorrendben jelennek meg:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    »more«:true|false,
    »batches«:
            [{
                »batchId«: »{uuid}«,
                »country«: »XY«,
                »date«: »2021-11-01T00:00:00Z«
                »deleted«: true | false
            }, ..
            ]
}
```

([1]) Az elavult azt jelenti, hogy ezt a funkciót az új végrehajtások tekintetében nem kell figyelembe venni, de használata a meglévő végrehajtások esetében egy jól meghatározott időpontig támogatott.

▼M3

Megjegyzés: Az eredmény alapértelmezés szerint 1 000 találatra korlátozódik. Ha a „more” (több) megjelölés igazra van beállítva, a válasz azt jelzi, hogy több tétel is letölthető. Több elem letöltéséhez az ügyfélnek az If-Modified-Since fejlécet az utolsó beérkezett bejegyzés dátumánál nem korábbi időpontra kell beállítania.

A válasz a következő szerkezetű JSON tömböt tartalmazza:

Mező	Meghatározás
more	Boolean megjelölés, ami azt jelzi, hogy több tétel is elérhető.
batches	Meglévő tételek tömbje.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Országkód ISO 3166
date	ISO 8601 UTC-dátum. A tétel hozzáadásának vagy törlésének dátuma.
deleted	boolean. Igaz, ha törölve van. Ha a törölt megjelölés van beállítva, a bejegyzés 7 nap elteltével véglegesen eltávolítható a lekérdezési eredmények közül.

9.5.1.2.1.1. Válaszkódok

Kód	Leírás
200	Minden ok.
204	Nincs elérhető tartalom, ha nincs egyezés az „If-Modified-Since” fejléc tartalmával.

A kérelem fejléce

Fejléc	Kötelező	Leírás
If-Modified-Since	Igen	Ez a fejléc az utolsó letöltött dátumot tartalmazza, hogy kizárólag a legújabb találatok legyenek elérhetők. Az első rákeresésnél a »2021-06-01T00:00:00Z« fejlécet kell beállítani.

9.5.1.2.2. A tétel letöltési végpontja

A tételek tartalmazzák az igazolványazonosítók listáját:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

»country«: »XY«,

»expires«: »2022-11-01T00:00:00Z«,

▼M3

»kid«:»23S+33f=«,

»hashType«:»SIGNATURE«,

»entries«:[{

»hash«:»e2e2e2e2e2e2e2e2«

}, ..]

}

A válasz egy CMS-t, többek között egy aláírást tartalmaz, melynek egyeznie kell az ország NB_{UP} tanúsítványával. A JSON tömb valamennyi eleme a következő szerkezetet tartalmazza:

Mező	Kötelező	Típus	Meghatározás
expires	Igen	String	Az a dátum, amikor a tétel eltávolítható. ISO 8601 UTC-dátum/-idő
country	Igen	String	Országkód ISO 3166
hashType	Igen	String	A megadott bejegyzések hash típusa (lásd: Hash típusok)
entries	Igen	JSON Object Array	Lásd a Bejegyzések táblázatát
kid	Igen	String	A DCC aláírásához használt DSC base64 szerint kódolt KID-je. Ha a KID nem ismert, akkor az UNKNOWN_KID' karakterlánc használható (a ' kivételével).

Megjegyzések:

— A tételeket lejárati nap és DSC szerint kell csoportosítani. Valamennyi tételnek egyidejűleg kell lejárnia, és azokat ugyanazzal a kulccsal kell aláírni.

— A lejárat időpontja az UTC szerinti dátum/idő, mivel az EU–DCC globális rendszer, melyben egyértelműen meghatározott időt kell használni.

— A véglegesen visszavont DCC lejárati időpontjaként a DCC aláírására használt megfelelő DSC lejárati időpontját vagy a visszavont DCC lejárati időpontját kell megjelölni (ez utóbbi esetben a felhasznált NumericDate/epoch időket az UTC időzónában lévőnek kell tekinteni).

— A nemzeti backend (NB) törli az elemeket a visszavonási listáról, amint elérkezik a **lejárat** napja.

— Az NB törölhet tételeket a saját visszavonási listájáról abban az esetben, ha a DCC aláírásához használt **kid** vissza lett vonva.

▼**M3**

9.5.1.2.2.1. Bejegyzések

Mező	Kötelező	Típus	Meghatározás
hash	Igen	String	A base64 karakterláncként kódolt SHA256 hash első 128 bitje

Megjegyzés: A bejegyzések objektuma jelenleg csak hash-t tartalmaz, de ahhoz, hogy összeegyeztethető legyen a jövőbeli változásokkal, a JSON tömb helyett egy objektum került kiválasztásra.

9.5.1.2.2.2. Válaszkódok

Kód	Leírás
200	Minden ok.
410	A tétel el lett távolítva. A tétel törölhető a nemzeti backendből.

9.5.1.2.2.3. Válaszfejlécek

Fejléc	Leírás
ETag	Tétel ID.

9.5.1.2.3. A tétel feltöltési végpontja

A feltöltés ugyanazon a végponton keresztül, a POST igével történik:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

{

»country«: »XY«,

»expires«: »2022-11-01T00:00:00Z«,

»kid«:»23S+33f=«,

»hashType«:»SIGNATURE«,

»entries«:[{

»hash«:»e2e2e2e2e2e2e2e2«

}, ..]

}

A tétel aláírásához az NB_{UP} tanúsítványt kell használni. Az átjáró ellenőrzi, hogy az aláírást valóban az adott *ország* NB_{UP} tanúsítványával rögzítették-e. Ha az aláírás ellenőrzése sikertelen, meghiúsul a feltöltés.

MEGJEGYZÉS: Valamennyi tétel megváltoztathatatlan, a feltöltés után nem módosítható. A tételt ugyanakkor lehet törölni a rendszerből. A rendszer minden törölt tétel azonosítóját tárolja, és az azzal megegyező azonosítóval rendelkező új tétel feltöltése elutasításra kerül.

▼M3

9.5.1.2.4. A tétel törlési végpontja

A tétel ugyanazon végponton keresztül, a DELETE igével törölhető:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

»batchId«: »...«

}

vagy a kompatibilitás érdekében a tétel a következő végponttal, a POST igével is törölhető:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

»batchId«: »...«

}

9.6. *API-védelem/általános adatvédelmi rendelet*

Ez a szakasz az (EU) 2021/953 rendelet személyes adatok kezelésére vonatkozó rendelkezéseinek való megfelelést szolgáló végrehajtási intézkedéseket határozza meg.

9.6.1. Meglévő hitelesítés

Az átjáró jelenleg az NB_{TLS} tanúsítványt használja az átjáróhoz csatlakozó országok hitelesítésére. Ez a hitelesítés alkalmazható az átjáróhoz csatlakozott ország azonosítására. Az azonosító ezt követően felhasználható a hozzáférés-ellenőrzés végrehajtására.

9.6.2. Hozzáférés-ellenőrzés

A személyes adatok jogszerű kezelése érdekében az átjáró hozzáférés-ellenőrzési mechanizmust vezet be.

Az átjáró a hozzáférés-ellenőrzési listát a szerepköralapú biztonsággal összekapcsolva hajtja végre. Ebben a rendszerben két táblázatot kell működtetni: az egyik táblázat megadja, hogy mely szerepkörök mely tevékenységeket milyen erőforrásokhoz rendelhetnek, a másik táblázat pedig azt ismerteti, hogy mely szerepkörök mely felhasználókhoz vannak rendelve.

Az e dokumentumban előírt ellenőrzések végrehajtásához három szerepkör szükséges, amelyek a következők:

RevocationListReader

RevocationUploader

RevocationDeleter

▼**M3**

A következő végpontok ellenőrzik, hogy a felhasználó rendelkezik-e a RevocationListReader szerepkörrel; ha igen, hozzáférést kell biztosítani, ha nem, akkor a HTTP 403 Forbidden válaszüzenetet kell adni:

GET/revocation-list/

GET/revocation-list/{batchId}

A következő végpontok ellenőrzik, hogy a felhasználó rendelkezik-e a RevocationUploader szerepkörrel; ha igen, hozzáférést kell biztosítani, ha nem, akkor a HTTP 403 Forbidden válaszüzenetet kell adni:

POST/revocation-list

A következő végpontok ellenőrzik, hogy a felhasználó rendelkezik-e a RevocationDeleter szerepkörrel; ha igen, hozzáférést kell biztosítani, ha nem, akkor a HTTP 403 Forbidden válaszüzenetet kell adni:

DELETE/revocation-list

POST/revocation-list/delete

Az átjáró megbízható módszert biztosít arra, hogy a rendszergazdák oly módon tudják kezelni a felhasználókhoz rendelt szerepköröket, melynek révén csökken az emberi hibák esélye, ugyanakkor nem hárul több teher a funkcionális rendszergazdákra.

▼M1

II. MELLÉKLET

AZ UNIÓS DIGITÁLIS COVID-IGAZOLVÁNY KITÖLTÉSÉRE VONATKOZÓ SZABÁLYOK

Az e mellékletben meghatározott értékkészletekre vonatkozó általános szabályok célja a szemantikai szintű interoperabilitás biztosítása; e szabályok lehetővé teszik az uniós digitális Covid-igazolvány egységes technikai végrehajtását. Az e mellékletben szereplő elemek az (EU) 2021/953 rendeletben meghatározott három különböző helyzet (oltás/tesztelés/gyógyulás) esetében használhatók. Ez a melléklet csak azokat az elemeket sorolja fel, amelyek esetében a kódolt értékkészletek révén szemantikai szabványosításra van szükség.

A kódolt elemek nemzeti nyelvre történő lefordítása a tagállamok felelőssége.

Az alábbi értékkészlet-leírásokban nem említett adatmezők esetében a kódolást az V. melléklet ismerteti.

Ha bármely okból az alább felsorolt, előnyben részesített kódrendszerek nem alkalmazhatók, más nemzetközi kódrendszerek is használhatók, és tanácsot kell adni arra vonatkozóan, hogyan kell a kódokat a másik kódrendszertől az előnyben részesített kódrendszerhez hozzárendelni. Kivételes esetekben tartalékmechanizmusként használható szöveg (megjelenített nevek), ha a meghatározott értékkészletekben nem áll rendelkezésre megfelelő kód.

A rendszerükben más kódolást alkalmazó tagállamoknak ezeket a kódokat hozzá kell rendelniük a leírt értékkészletekhez. Az ilyen hozzárendelésekért a tagállamok felelősek.

►M4 Mivel az e mellékletben előírt kódolási rendszereken alapuló egyes értékkészletek – például azok, amelyek az oltóanyag és az antigén teszt kódolására vonatkoznak – gyakran változnak, a Bizottságnak az e-egészségügyi hálózat és az Egészségügyi Biztonsági Bizottság támogatásával rendszeresen közzé kell tennie és frissítenie kell ezeket. ◄ A frissített értékkészleteket közzé kell tenni a Bizottság megfelelő honlapján, valamint az e-egészségügyi hálózat honlapján. A változtatásokat archiválni kell.

1. **Célzott betegség vagy kórokozó/a betegség vagy kórokozó, amelyből a birtokos felgyógyult: Covid19 (SARS-CoV-2 vagy annak egyik variánsa)**

   Az 1., 2. és 3. igazolványban használandó.

   A következő kódot kell használni:

Kód	Megjelenítés	Kódrendszer neve	Kódrendszer webcíme (URL)	Kódrendszer szervezeti azonosítója (OID)	Kódrendszer verziója
840539006	COVID-19	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

2. **Covid19-oltóanyag vagy profilaxis**

   Előnyben részesített kódrendszer: SNOMED CT vagy ATC osztályozás.

   Az 1. igazolványban használandó.

   Az előnyben részesített kódrendszerekből a következő kódokat kell használni: SNOMED CT-kód: 1119305005 (SARS-CoV-2 antigén oltóanyag), 1119349007 (SARS-CoV-2 mRNS oltóanyag) vagy J07BX03 (Covid19-oltóanyagok).

   A Bizottságnak az e-egészségügyi hálózat támogatásával rendszeresen közzé kell tennie és frissítenie kell az e szakaszban megállapított kódrendszerek alapján használandó kódokat meghatározó értékkészletet. Az értékkészletet ki kell bővíteni, ha új oltóanyagtípusokat fejlesztenek ki és alkalmaznak.

▼M1

3. **Covid19-oltóanyag gyógyszerkészítmény**

Előnyben részesített kódrendszerek (az előnyben részesítés sorrendjében):

— Gyógyszerkészítmények Uniós Nyilvántartása az uniós szintű engedéllyel rendelkező oltóanyagokra vonatkozóan (engedélyszámok);

— egy olyan globális oltóanyag-nyilvántartás, mint amelyet az Egészségügyi Világszervezet hozhat létre;

— egyéb esetekben az oltóanyag gyógyszer neve. Ha a név üres helyeket is tartalmaz, azokat kötőjellel (-) kell helyettesíteni.

Az értékkészlet neve: Oltóanyag.

Az 1. igazolványban használandó.

Az előnyben részesített kódrendszerben használandó kódra példa az EU/1/20/1528 (Comirnaty). Példa a kódként használandó oltóanyag nevére: Sputnik-V (Sputnik V helyett).

A Bizottságnak az e-egészségügyi hálózat támogatásával rendszeresen közzé kell tennie és frissítenie kell az e szakaszban megállapított kódrendszerek alapján használandó kódokat meghatározó értékkészletet.

Az oltóanyagokat a közzétett értékkészletben meglévő kód használatával kell kódolni, még akkor is, ha nevük különböző országokban eltérő. Ennek az az oka, hogy nincs olyan globális oltóanyag-nyilvántartás, amely lefedné a jelenleg használatban lévő összes oltóanyagot. Példa:

— A „CoVID-19 Vaccine Moderna Intramuscular Injection” elnevezésű oltóanyag esetében, amely a Spikevax oltóanyag japán neve, az EU/1/20/1507 kódot kell használni, mivel ennek az oltóanyagnak ez a neve az EU-ban.

Ha ez egy konkrét esetben nem lehetséges vagy tanácsos, külön kódot adnak meg a közzétett értékkészletben.

▼M4

Ha az uniós digitális Covid-igazolványt használó ország úgy dönt, hogy a folyamatban lévő klinikai vizsgálatok során oltási igazolványokat állít ki a klinikai vizsgálatok résztvevői számára, az oltóanyagot a következő mintának megfelelően kell kódolni:

CT_*clinical-trial-identifier*

Amennyiben a klinikai vizsgálatot regisztrálták a klinikai vizsgálatok uniós nyilvántartásában (EU-CTR), az ebből a nyilvántartásból származó klinikai vizsgálati azonosítót kell használni. Egyéb esetekben más nyilvántartásokból (például klinikai vizsgálatok.gov vagy Australian New Zealand Clinical Trials Registry) származó azonosítók is használhatók.

A klinikai vizsgálat azonosítójának tartalmaznia kell egy olyan előtagot, amely lehetővé teszi a klinikai vizsgálatok nyilvántartásának azonosítását (például EUCTR a klinikai vizsgálatok uniós nyilvántartása esetében, NCT a clinicaltrials.gov esetében, ACTRN az Australian New Zealand Clinical Trials Registry esetében).

Amennyiben a Bizottság iránymutatást kapott az Egészségügyi Biztonsági Bizottságtól, az Európai Betegségmegelőzési és Járványvédelmi Központtól (ECDC) vagy az Európai Gyógyszerügynökségtől (EMA) a klinikai vizsgálatok tárgyát képező Covid19-oltóanyagok tekintetében igazolványok elfogadásáról, az iránymutatást vagy az értékkészletet meghatározó dokumentum részeként, vagy külön kell közzétenni.

▼M1

4. **A Covid19-oltóanyag forgalombahozatali engedélyének jogosultja vagy az oltóanyag gyártója**

Előnyben részesített kódrendszer:

— az EMA (SPOR rendszer ISO IDMP-hez) szerinti szervezetkód;

— egy olyan globális oltóanyag forgalombahozatali engedély jogosult- vagy oltóanyaggyártó-nyilvántartás, mint amelyet az Egészségügyi Világszervezet hozhat létre;

— egyéb esetekben a szervezet neve. Ha a név üres helyeket is tartalmaz, azokat kötőjellel (-) kell helyettesíteni.

Az 1. igazolványban használandó.

Az előnyben részesített kódrendszerben használandó kódra példa az ORG-100001699 (AstraZeneca AB). Példa a kódként használandó szervezet nevére: Sinovac-Biotech (Sinovac Biotech helyett).

A Bizottságnak az e-egészségügyi hálózat támogatásával rendszeresen közzé kell tennie és frissítenie kell az e szakaszban megállapított kódrendszerek alapján használandó kódokat meghatározó értékkészletet.

Azonos forgalombahozataliengedély-jogosult vagy azonos gyártó különböző fióktelepei a közzétett értékkészletben meglévő kódot használnak.

Főszabály szerint ugyanazon oltóanyagtermék esetében a forgalombahozatali engedély jogosultjára vonatkozó kódot kell használni az EU-ban, mivel még nincs nemzetközileg elfogadott nyilvántartás az oltóanyaggyártókra vagy a forgalombahozatali engedélyek jogosultjaira. Példák:

— A „Pfizer AG” szervezet esetében, amely a Svájcban használt „Comirnaty” oltóanyag forgalombahozatali engedély jogosultja, a BioNTech Manufacturing GmbH-ra utaló ORG-100030215 kódot kell használni, mivel az utóbbi a Comirnaty forgalombahozatali engedély jogosultja az EU-ban.

— A „Zuellig Pharma” szervezet esetében, amely a Fülöp-szigeteken használt Moderna (Spikevax) Covid19-oltóanyag forgalombahozatali engedély jogosultja, a Moderna Biotech Spain S.L.-re utaló ORG-100031184 kódot kell használni, mivel az utóbbi a Spikevax forgalombahozatali engedély jogosultja az EU-ban.

Ha ez egy konkrét esetben nem lehetséges vagy tanácsos, külön kódot adnak meg a közzétett értékkészletben.

▼M4

Ha az uniós digitális Covid-igazolványt használó ország úgy dönt, hogy a folyamatban lévő klinikai vizsgálatok során oltási igazolványokat állít ki a klinikai vizsgálatok résztvevői számára, a vakcina forgalombahozatali engedélyének jogosultját vagy a vakcina gyártóját az értékkészletben megjelölt érték felhasználásával kell kódolni, ha az rendelkezésre áll. Egyéb esetekben az oltóanyag forgalombahozatali engedélyének jogosultját vagy az oltóanyag gyártóját a 3. szakaszban (Oltóanyag gyógyszerkészítmény) leírt szabály alkalmazásával kell kódolni (CT_*clinical-trial-identifier*).

▼M1

5. **A dózisok sorszáma és teljes száma**

Az 1. igazolványban használandó.

Két mező:

(1) a Covid19-oltóanyagdózisokon belüli sorszám (N);

(2) a dózisok teljes száma (C).

5.1. *Elsődleges vakcinázási sorozat*

Ha az adott személy az elsődleges vakcinázási sorozat során kap dózisokat – vagyis abban a vakcinázási sorozatban, amelynek célja, hogy a kezdeti szakaszban megfelelő védelmet nyújtson – a (C) a standard elsődleges vakcinázási sorozatok dózisainak teljes számát tükrözi (pl. a beadott oltóanyag típusától függően 1 vagy 2). Ez magában foglalja rövidebb sorozat (C=1) alkalmazásának lehetőségét is, ha az adott tagállam által alkalmazott vakcinázási protokoll előírása szerint a két dózist tartalmazó oltóanyagok esetében egy dózist kell beadni a korábban SARS-CoV-2-vel fertőzött személyeknek. A befejezett vakcinázási sorozatot ezért N/C = 1 jelzi. Például:

— az 1/1 az egyadagos elsődleges oltási folyamat befejezését, vagy a tagállam által alkalmazott vakcinázási protokollnak megfelelően a gyógyult személyeknek a kétadagos oltóanyagból beadott egy adagból álló elsődleges oltási folyamat befejezését jelzi;

— a 2/2 a 2 adagból álló elsődleges vakcinázási sorozat befejezését jelzi.

Ha az elsődleges vakcinázási sorozatot kibővítik, például súlyosan meggyengült immunrendszerű személyek esetében, vagy ha az elsődleges dózisok között ajánlott időközt nem tartották be, az ilyen adagokat az 5.2. szakasz szerinti kiegészítő dózisként kell kódolni.

▼M2

5.2. *Erősítő adagok*

Amennyiben a személy az alapoltási sorozatot követően kap booster adagokat, ezen booster adagokat a megfelelő igazolványokban az alábbiak szerint kell feltüntetni:

— a 2/1 az egyadagos alapoltást követő dózis beadását, vagy a tagállam által alkalmazott vakcinázási protokollnak megfelelően a gyógyult személyeknek a kétadagos oltóanyagból beadott egy adagból álló alapoltás befejezését követő booster adag beadását jelzi. Ezt követően az első booster adag után beadott (X) adagokat a (2+X)/(1) > 1 (például 3/1) jelzi,

— a 3/3 a 2 adagból álló alapoltási sorozat befejezését követő booster adag beadását jelzi. Ezt követően az első booster adag után beadott (X) dózist (3+X)/(3+X) = 1 (például 4/4) értékkel kell jelezni.

A tagállamok 2022. február 1-jéig végrehajtják az e szakaszban meghatározott kódolási szabályokat.

A tagállamok automatikusan vagy az érintett személyek kérésére újra kiállítják azokat az igazolványokat, amelyekben az egy adagból álló alapoltást követő booster adag beadását oly módon kódolják, hogy az nem megkülönböztethető az alapoltási sorozat befejezésétől.

▼M2

E melléklet alkalmazásában a „booster adagokra” való hivatkozásokat úgy kell értelmezni, hogy azok magukban foglalják a standard alapoltási sorozat befejezését követően nem megfelelő immunválaszt adó személyek hatékonyabb védelme érdekében alkalmazott kiegészítő dózisokat is. Az (EU) 2021/953 rendelettel létrehozott jogi kereten belül a tagállamok intézkedéseket hozhatnak azon veszélyeztetett csoportok helyzetének kezelésére, akik elsőbbséggel kaphatnak kiegészítő dózisokat. Például ha valamely tagállam úgy dönt, hogy csak a népesség bizonyos alcsoportjai számára ad be kiegészítő dózisokat, az (EU) 2021/953 rendelet 5. cikkének (1) bekezdése szerint dönthet úgy, hogy kizárólag kérésre, nem pedig automatikusan állít ki az ilyen kiegészítő dózisok beadását feltüntető oltási igazolványokat. Amennyiben ilyen intézkedésekre kerül sor, a tagállamok tájékoztatják az érintett személyeket erről, valamint arról, hogy továbbra is használhatják a standard alapoltási sorozatok befejezését követően kapott igazolványt.

▼M1

6. **Az oltás beadásának vagy a teszt elvégzésének helye szerinti tagállam vagy harmadik ország**

Előnyben részesített kódrendszer: ISO 3166-országkódok.

Az 1., 2. és 3. igazolványban használandó.

Az értékkészlet tartalma: Az FHIR-ben ((http://hl7.org/fhir/ValueSet/iso3166-1-2) meghatározott értékkészletként rendelkezésre álló kétbetűs kódok teljes jegyzéke. Ha az oltást vagy a tesztet nemzetközi szervezet (például az UNHCR vagy a WHO) végezte el, és az országra vonatkozó információ nem áll rendelkezésre, a szervezet kódját kell használni. Ezeket a kiegészítő kódokat a Bizottságnak az e-egészségügyi hálózat támogatásával rendszeresen közzé kell tennie és frissítenie kell.

7. **A teszt típusa**

A 2. és 3. igazolványban kell használni, amennyiben felhatalmazáson alapuló jogi aktus útján támogatást nyújtanak a NAAT-tól eltérő típusú teszteken alapuló gyógyultságra vonatkozó igazolványok kibocsátásához.

Az alábbi kódokat kell használni.

Kód	Megjelenítés	Kódrendszer neve	Kódrendszer webcíme (URL)	Kódrendszer szervezeti azonosítója (OID)	Kódrendszer verziója
LP6464-4	Nukleinsav-amplifikációs teszt szondával történő detektálással	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69
LP217198-3	Gyors immunvizsgálat	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69

▼M4

Az LP217198–3 kódot (gyors immunvizsgálat) kell használni mind az antigén gyorstesztek, mind a laboratóriumi antigénvizsgálatok jelölésére.

▼M1

8. **Az alkalmazott teszt gyártójának neve és a teszt kereskedelmi neve (NAAT-tesztnél választható)**

A 2. igazolványban használandó.

▼M4

Az értékkészletnek tartalmaznia kell a Covid19 antigén teszteknek a 2021/C 24/01 tanácsi ajánlás alapján létrehozott és az Egészségügyi Biztonsági Bizottság által jóváhagyott közös és aktualizált jegyzékében felsorolt antigén tesztek kiválasztását. A jegyzéket a JRC tartja fenn a Covid19 in vitro diagnosztikai eszközök és tesztmódszerek alábbi adatbázisában: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

▼M1

Ehhez a kódrendszerhez olyan releváns mezőket kell használni, mint például a teszteszköz azonosítója, a teszt és a gyártó neve, a JRC strukturált formátumának megfelelően, amely az alábbi weboldalon érhető el: https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Teszteredmény**

A 2. igazolványban használandó.

A következő kódokat kell használni:

Kód	Megjelenítés	Kódrendszer neve	Kódrendszer webcíme (URL)	Kódrendszer szervezeti azonosítója (OID)	Kódrendszer verziója
260415000	Nem kimutatott	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31
260373001	Kimutatott	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

▼B

III. MELLÉKLET

AZ EGYEDI IGAZOLVÁNYAZONOSÍTÓ KÖZÖS SZERKEZETE

1. **Bevezetés**

Minden egyes uniós digitális Covid-igazolványnak (DCC) tartalmaznia kell egy egyedi igazolványazonosítót (UCI), amely támogatja a DCC-k interoperabilitását. Az UCI az igazolvány ellenőrzésére használható. Az UCI végrehajtásáért a tagállamok felelősek. Az UCI az igazolvány valódiságának ellenőrzésére szolgáló eszköz, és adott esetben egy nyilvántartási rendszerhez (például egy IIS-hez) vezető link. Ezek az azonosítók azt is lehetővé teszik, hogy a tagállamok (papíralapú és digitális) állításokat tegyenek arra vonatkozóan, hogy az egyéneket beoltották vagy tesztelték.

2. **Az egyedi igazolványazonosító kialakítása**

Az UCI-nak olyan közös struktúrát és formátumot kell követnie, amely megkönnyíti az információk emberi és/vagy gépi értelmezését, és kapcsolódhat olyan elemekhez, mint az oltás helye szerinti tagállam, maga az oltóanyag és egy tagállam-specifikus azonosító. Rugalmasságot biztosít a tagállamok számára a formátum tekintetében, az adatvédelmi jogszabályok teljeskörű tiszteletben tartása mellett. Az egyes elemek sorrendje meghatározott hierarchiát követ, amely lehetővé teszi a blokkok jövőbeli módosítását a szerkezeti integritás fenntartása mellett.

Az UCI kialakítására vonatkozó lehetséges megoldások olyan spektrumot alkotnak, amelyben a modularitás és az ember általi értelmezhetőség a két fő diverzifikációs paraméter és az egyik alapvető jellemző:

— modularitás: annak foka, hogy a kód milyen mértékben áll szemantikai szempontból eltérő információkat tartalmazó, különálló építőelemekből,

— ember általi értelmezhetőség: annak foka, hogy a kód milyen mértékben bír jelentéssel, vagy mennyire értelmezhető az azt olvasó ember által,

— globális egyediség: az ország- vagy hatóságazonosító kezelése megfelelő; és az egyes országoktól (hatóságoktól) elvárható, hogy a névtartomány szegmensüket jól kezeljék, úgy, hogy sohasem hasznosítják újra és nem bocsátják ki újra az azonosítókat. Ezek kombinációja biztosítja az egyes azonosítók globális egyediségét.

▼M1

3. **Általános követelmények**

Az UCI tekintetében a következő átfogó követelményeknek kell teljesülniük:

1. Karakterkészlet: csak a nagybetűs US-ASCII alfanumerikus karakterek („A”-tól „Z”-ig, „0”-tól „9”-ig) megengedettek; az RFC3986 ([1]), szabvány szerinti, elválasztásra szolgáló további különleges karakterekkel, azaz {'/','#',':'};

2. Maximális hosszúság: a tervezők 27–30 karakter hosszúságra törekednek ([2]);

3. Verzió előtag: ez jelzi az UCI-séma verzióját. A dokumentum jelen verziója esetében a verzió előtagja „01”; a verzió előtag két számjegyből áll.

([1]) rfc3986 (ietf.org)

([2]) A QR-kódokkal történő végrehajtáshoz a tagállamok fontolóra vehetik, hogy további karakterkészletet is felhasználhatnak legfeljebb 72 karakter terjedelemben (beleértve magának az azonosítónak a 27–30 karakterét is) más információk továbbítására. Ezen információk előírását a tagállamok határozzák meg.

▼M1

4. Ország előtag: az országkódot az ISO 3166-1 határozza meg. A hosszabb kódok (pl. 3 és annál több karakter) (például „UNHCR”) későbbi használatra vannak fenntartva.

5. Kód utótag/Ellenőrző összeg:

5.1. A tagállamok ellenőrző összeget használhatnak, ha valószínűsíthető, hogy továbbítás, (emberi) átírás vagy egyéb sérülés következhet be (azaz a nyomtatásban történő használat esetén).

5.2. Az igazolvány validálásához nem kell az ellenőrző összegre támaszkodni, és az nem képezi technikailag az azonosító részét, hanem a kód sértetlenségének ellenőrzésére szolgál. Ennek az ellenőrző összegnek a teljes UCI ISO-7812-1 (LUHN-10) ([1]) szabvány szerinti összefoglalójának kell lennie digitális/vezetékes továbbítási formátumban. Az ellenőrző összeget „#” karakter választja el az UCI többi részétől.

Biztosítani kell a visszamenőleges kompatibilitást: azok a tagállamok, amelyek idővel megváltoztatják azonosítóik szerkezetét (a jelenleg v1-ként meghatározott fő változaton belül), biztosítják, hogy bármely két azonos azonosító ugyanazt az oltási igazolványt/állítást takarja. Más szavakkal, a tagállamok nem hasznosíthatják újra az azonosítókat.

▼B

4. **Az oltási igazolványok egyedi igazolványazonosítóinak lehetőségei**

Az e-egészségügyi hálózatnak az ellenőrizhető oltási igazolványokra és az alapvető interoperabilitási elemekre vonatkozó iránymutatásai ([2]) különböző lehetőségeket biztosítanak a tagállamok és más felek számára, amelyek a különböző tagállamokban párhuzamosan létezhetnek. A tagállamok az UCI-séma különböző verzióiban alkalmazhatják ezeket a különböző lehetőségeket.

([1]) A Luhn mod N algoritmus a Luhn-algoritmus (más néven mod 10 algoritmus) kiterjesztése, amely numerikus kódokat használ, és amelyet például a hitelkártyák ellenőrző összegének kiszámításához használnak. A kiterjesztés lehetővé teszi, hogy az algoritmus bármilyen alapértéksorral (esetünkben alfa karakterekkel) működjön.

([2]) https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

▼B

IV. MELLÉKLET

A NYILVÁNOS KULCSOK TANÚSÍTVÁNYAIRA VONATKOZÓ IRÁNYÍTÁSI SZABÁLYOK

1. Bevezetés

Az uniós digitális Covid-igazolványok (DCC-k) aláírási kulcsainak tagállamok közötti biztonságos és megbízható cseréjét az uniós digitális Covid-igazolvány átjárója (DCCG) valósítja meg, amely a nyilvános kulcsok központi adattáraként működik. A DCCG használatával a tagállamok közzétehetik a digitális Covid-igazolványok aláírásához használt titkos kulcsoknak megfelelő nyilvános kulcsokat. Az igénybe vevő tagállamok a DCCG-t arra használhatják, hogy kellő időben naprakész nyilvánoskulcs-anyagokat készítsenek. Később a DCCG kiterjeszthető a tagállamok által szolgáltatott megbízható kiegészítő információk cseréjére, például a DCC-kre vonatkozó validálási szabályokra. A DCC-keret bizalmi modellje nyilvános kulcsú infrastruktúra (PKI). Minden tagállam egy vagy több országos aláíró hitelesítésszolgáltatót (CSCA) tart fenn, amelyek tanúsítványai viszonylag hosszú ideig élnek. A tagállam döntése alapján a CSCA lehet ugyanaz vagy eltérő, mint a géppel olvasható úti okmányokhoz használt CSCA. A CSCA nyilvános kulcstanúsítványokat bocsát ki a nemzeti, rövid élettartamú dokumentum aláírók (azaz a DCC-k aláírói) számára, amelyeket dokumentum aláíró tanúsítványnak (DSC) neveznek. A CSCA olyan bizalmi horgonyként működik, amely lehetővé teszi a szolgáltatást igénybe vevő tagállamok számára, hogy a rendszeresen változó DSC-tanúsítványok hitelességének és sértetlenségének validálására használják a CSCA-t. A validálást követően a tagállamok ezeket a tanúsítványokat (vagy csak az azokban található nyilvános kulcsokat) átadhatják DCC ellenőrzési alkalmazásaiknak. A CSCA-k és a DSC-k mellett a DCCG a hitelesítés alapjaként, valamint a tagállamok és a DCCG közötti kommunikációs csatornák sértetlensége biztosításának eszközeként a PKI-re is támaszkodik a tranzakciók hitelesítése, az adatok aláírása érdekében.

A digitális aláírások felhasználhatók az adatok sértetlenségének és hitelességének elérésére. A nyilvános kulcsú infrastruktúrák a nyilvános kulcsok ellenőrzött szervezetekhez (vagy kibocsátókhoz) való kötésével teremtenek bizalmat. Erre azért van szükség, hogy a többi résztvevő ellenőrizhesse a kommunikációs partner adatforrását és személyazonosságát, és dönthessen a bizalomról. A DCCG-ben a hitelesség érdekében több nyilvános kulcsú tanúsítványt használnak. A jelen melléklet meghatározza, hogy a tagállamok közötti széles körű interoperabilitás érdekében milyen nyilvános kulcsú tanúsítványokat használnak és hogyan kell azokat kialakítani. Részletesebb tájékoztatást nyújt a szükséges nyilvánoskulcs-tanúsítványokról, és iránymutatást ad a tanúsítványmintákról és az érvényességi időszakokról azon tagállamok számára, amelyek saját CSCA-t kívánnak működtetni. Mivel a DCC-knek meghatározott időtartamig ellenőrizhetőknek kell lenniük (a kibocsátástól kezdődően, egy adott idő elteltével lejárva), meg kell határozni egy ellenőrzési modellt a nyilvánoskulcs-tanúsítványokon és a DCC-ken alkalmazott valamennyi aláírásra vonatkozóan.

2. Terminológia

Az alábbi táblázat a jelen mellékletben használt rövidítéseket és terminológiát tartalmazza.

Kifejezés	Meghatározás
Tanúsítvány	Vagy nyilvánoskulcs-tanúsítvány. Egy szervezet nyilvános kulcsát tartalmazó X.509 v3 tanúsítvány

▼B

Kifejezés	Meghatározás
CSCA	Országos aláíró hitelesítésszolgáltató
DCC	Uniós digitális Covid-igazolvány. Oltásra, tesztelésre vagy gyógyulásra vonatkozó információkat tartalmazó aláírt digitális dokumentum
DCCG	Uniós digitális Covid-igazolvány átjáró. Ez a rendszer a DSC-k tagállamok közötti cseréjére szolgál
$DCCG_{TA}$	A DCCG bizalmi horgonya. A megfelelő titkos kulcsot az összes CSCA-tanúsítvány jegyzékének offline aláírásához használják
$DCCG_{TLS}$	A DCCG TLS szerver tanúsítványa
DSC	Dokumentum aláíró tanúsítvány. A tagállam dokumentum-aláíró hatóságának nyilvános kulcsú tanúsítványa (például DCC-k aláírására engedélyezett rendszer). Ezt a tanúsítványt a tagállam CSCA-ja bocsátja ki
EC-DSA	Elliptikus görbéken alapuló digitális aláírási algoritmus. Elliptikus görbéken alapuló kriptográfiai aláírás algoritmus
Tagállam	Az Európai Unió tagállama
mTLS	Kölcsönös TLS. Kölcsönös hitelesítéssel rendelkező szállítási réteg biztonsági protokoll
NB	Egy tagállam nemzeti backendje
NB_{CSCA}	A tanúsítvány CSCA-tanúsítványa (lehet egynél több)
NB_{TLS}	Egy nemzeti backend TLS ügyfélhitelesítési tanúsítványa
NB_{UP}	A nemzeti backend által a DCCG-be feltöltött adatcsomagok aláírásához használt tanúsítvány
PKI	Nyilvános kulcsú infrastruktúra. Nyilvánoskulcs-tanúsítványokon és tanúsítványokért felelős hatóságokon alapuló bizalmi modell
RSA	Egész számok faktorizálásán alapuló aszimmetrikus kriptográfiai algoritmus, amelyet digitális aláírásra vagy aszimmetrikus titkosításra használnak

3. **DCCG kommunikációs folyamatok és biztonsági szolgáltatások**

Ez a szakasz áttekintést nyújt a DCCG-rendszer kommunikációs folyamatairól és biztonsági szolgáltatásairól. Meghatározza továbbá, hogy milyen kulcsokat és tanúsítványokat használnak a kommunikáció, a feltöltött információk, a DCC-k, valamint az összes hatályos CSCA-tanúsítványt tartalmazó, aláírt bizalmi jegyzék védelmére. A DCCG az aláírt adatcsomagok tagállamok közötti cseréjét lehetővé tevő adatközpontként működik.

▼B

A feltöltött adatcsomagokat a DCCG „az adott állapotban” bocsátja rendelkezésre, ami azt jelenti, hogy a DCCG nem ad hozzá és nem töröl DSC-ket a kapott csomagokból. A tagállamok nemzeti backendje (NB) számára lehetővé kell tenni a feltöltött adatok végpontok közötti sértetlenségének és hitelességének ellenőrzését. Emellett a nemzeti backendek és a DCCG kölcsönös TLS-hitelesítést fognak használni a biztonságos kapcsolat létrehozása érdekében. Ez kiegészíti a kicserélt adatokban szereplő aláírásokat.

3.1. *Hitelesítés és kapcsolat létesítése*

A DCCG kölcsönös hitelesítésű szállítási réteg biztonságot (TLS) használ a tagállam nemzeti backendje (NB) és a kapukörnyezet közötti hitelesített titkosított csatorna létrehozására. Ezért a DCCG TLS szervertanúsítvánnyal (rövidítve $DCCG_{TLS}$), a nemzeti backendek pedig TLS ügyféltanúsítvánnyal (rövidített NB_{TLS}) rendelkeznek. A tanúsítványminták az *5. szakaszban* találhatók. Minden nemzeti backend saját TLS tanúsítványt állíthat ki. Ez a tanúsítvány kifejezetten engedélyezőlistára kerül, és így azt egy megbízható nyilvános hitelesítésszolgáltató (például a CA böngészőfórum alapkövetelményeinek megfelelő hitelesítésszolgáltató), illetve egy nemzeti hitelesítésszolgáltató állíthatja ki, vagy önaláírt lehet. Minden tagállam felelős a saját nemzeti adataiért és a DCCG-vel való kapcsolat létrehozásához használt titkos kulcs védelméért. A „hozd a saját tanúsítványod” megközelítéshez egy jól meghatározott regisztrációs és azonosítási folyamatra, valamint a *4.1., a 4.2. és a 4.3. szakaszban* leírt visszavonási és megújítási eljárásokra van szükség. A DCCG egy engedélyezőlistát használ, amelyhez az NB-k TLS-tanúsítványait a sikeres regisztrációt követően adják hozzá. A DCCG-vel való biztonságos kapcsolatot csak azok az NB-k képesek létrehozni, amelyek az engedélyezőlistán szereplő tanúsítványnak megfelelő titkos kulccsal hitelesítik magukat. A DCCG egy TLS tanúsítványt is használ, amely lehetővé teszi a NB-k számára annak ellenőrzését, hogy valóban a „valódi” DCCG-vel teremtenek-e kapcsolatot, és nem valamiféle rosszhiszemű szervezettel, amely a DCCG-nek adja ki magát. A DCCG tanúsítványát a sikeres regisztrációt követően átadják az NB-knek. A $DCCG_{TLS}$ tanúsítványt egy nyilvánosan megbízható (valamennyi nagyobb böngészőben szereplő) CA bocsátja ki. A tagállamok feladata annak ellenőrzése, hogy a DCCG-vel való kapcsolatuk biztonságos-e (például a csatlakoztatott szerver $DCCG_{TLS}$ tanúsítvány ujjlenyomatának ellenőrzésével a regisztráció után megadottal összevetve).

3.2. *Országos aláíró hitelesítésszolgáltatók és a validálási modell*

A DCCG-keretrendszerben részt vevő tagállamoknak CSCA-t kell használniuk a DSC-k kiadásához. A tagállamok rendelkezhetnek egynél több CSCA-val, például regionális decentralizáció esetén. Minden tagállam igénybe veheti a meglévő hitelesítésszolgáltatókat, vagy létrehozhat egy külön (esetleg önaláírt) hitelesítésszolgáltatót a DCC-rendszer számára.

A tagállamoknak a hivatalos bevezetési eljárás során be kell mutatniuk CSCA-tanúsítványukat/tanúsítványaikat a DCCG-üzemeltetőnek. A tagállam sikeres regisztrációját követően (*további részletekért lásd a 4.1. szakaszt*) a DCCG üzemeltetője aktualizálja az aláírt bizalmi jegyzéket, amely tartalmazza a DCC-keretében aktív valamennyi CSCA-tanúsítványt. A DCCG-üzemeltető külön aszimmetrikus kulcspárt használ a bizalmi jegyzék és a tanúsítványok offline környezetben történő aláírására. A titkos kulcsot nem tárolják az online DCCG rendszerben, így az online rendszer sérelme nem teszi lehetővé, hogy a támadó veszélyeztesse a bizalmi listát. A megfelelő $DCCG_{TA}$ bizalmi horgony tanúsítványt a bevezetési folyamat során adják át a nemzeti backendeknek.

▼B

A tagállamok az ellenőrzési eljárásaikhoz lekérhetik a megbízhatósági jegyzéket a DCCG-ből. A CSCA az a hitelesítésszolgáltató, amely DSC-ket bocsát ki, ezért azoknak a tagállamoknak, amelyek többszintű CA-hierarchiát alkalmaznak (pl. gyökér CA -> CSCA -> DSC-k), meg kell jelölniük a DSC-ket kibocsátó alárendelt hitelesítésszolgáltatót. Ebben az esetben, ha egy tagállam egy meglévő hitelesítésszolgáltatót használ, a DCC-rendszer CSCA-n kívül mindent figyelmen kívül hagy, és csak a CSCA-t helyezi bizalmi horgonyként engedélyezőlistára (még akkor is, ha az egy alárendelt hitelesítésszolgáltató). Ez olyan, mint az ICAO-modell: csak pontosan két szintet tesz lehetővé – egy „gyökér” CSCA-t és egy kizárólag az adott CSCA által aláírt „levél” DSC-t.

Abban az esetben, ha egy tagállam saját CSCA-t működtet, a tagállam felelős a hitelesítésszolgáltató biztonságos működéséért és kulcskezeléséért. A CSCA a DSC-k bizalmi horgonyaként működik, ezért a CSCA titkos kulcsának védelme alapvető fontosságú a DCC környezetének sértetlensége szempontjából. A DCC PKI-n belüli ellenőrzési modell a héjmodell, amely szerint a tanúsítvány útvonalának validálásában szereplő valamennyi tanúsítványnak egy adott időpontban (azaz az aláírás validálásának időpontjában) érvényesnek kell lennie. Ezért a következő korlátozásokat kell alkalmazni:

— a CSCA nem állíthat ki olyan tanúsítványokat, amelyek hosszabb ideig érvényesek, mint magának a hitelesítésszolgáltatónak a tanúsítványa,

— a dokumentum aláíró nem írhat alá olyan dokumentumokat, amelyek hosszabb ideig érvényesek, mint maga a DSC,

— a saját CSCA-jukat működtető tagállamoknak meg kell határozniuk a CSCA-juk és valamennyi kiállított tanúsítvány érvényességi idejét, és gondoskodniuk kell a tanúsítványok megújításáról.

A *4.2. szakasz* tartalmazza az érvényességi időkre vonatkozó ajánlásokat.

3.3. *A feltöltött adatok sértetlensége és hitelessége*

A nemzeti backendek a DCCG használatával digitálisan aláírt adatcsomagokat tölthetnek fel és tölthetnek le a sikeres kölcsönös hitelesítést követően. Kezdetben ezek az adatcsomagok a tagállamok DSC-it tartalmazzák. Azt a kulcspárt, amelyet a nemzeti backend a DCCG-rendszerben feltöltött adatcsomagok digitális aláírásához használ, nemzeti backend-feltöltési kulcspárnak, a megfelelő nyilvánoskulcs-tanúsítványt pedig rövidítve NB_{UP} tanúsítványnak nevezik. Minden tagállam hozza a saját NB_{UP} tanúsítványát, amelyet lehet önaláírt, vagy kibocsáthatja egy meglévő hitelesítésszolgáltató, például egy nyilvános hitelesítésszolgáltató (azaz a tanúsítványokat a CAB-fórum alapkövetelményeinek megfelelően kiállító hitelesítésszolgáltató). A NB_{UP} tanúsítvány eltér a tagállam által használt bármely egyéb tanúsítványtól (amely lehet CSCA, TLS ügyfél vagy DSC).

A tagállamoknak az első regisztrációs eljárás során át kell adniuk a feltöltési tanúsítványt a DCCG-üzemeltetőnek (*további részletekért lásd a 4.1. szakaszt*). Minden tagállam felelős a saját nemzeti adataiért és köteles védeni a feltöltések aláírására használt titkos kulcsot.

Más tagállamok a DCCG által rendelkezésre bocsátott feltöltési tanúsítványok használatával ellenőrizhetik az aláírt adatcsomagokat. A DCCG a más tagállamok részére történő átadás előtt az NB feltöltési tanúsítvánnyal ellenőrzi a feltöltött adatok hitelességét és sértetlenségét.

▼B

3.4. *A DCCG műszaki felépítésére vonatkozó követelmények*

A DCCG műszaki felépítésére vonatkozó követelmények a következők:

— a DCCG kölcsönös TLS-hitelesítést alkalmaz az NB-kkel való hitelesített titkosított kapcsolat létrehozására. A DCCG ezért fenntartja a regisztrált NB_{TLS} ügyféltanúsítványok engedélyezőlistáját,

— a DCCG két különböző kulcspárral rendelkező két digitális tanúsítványt használ ($DCCG_{TLS}$ és $DCCG_{TA}$). A $DCCG_{TA}$ kulcspár titkos kulcsát offline tartják fenn (nem pedig a DCCG online összetevőin),

— a DCCG vezeti a $DCCG_{TA}$ titkos kulccsal aláírt NB_{CSCA} tanúsítványok bizalmi jegyzékét,

— a felhasznált titkosítóknak meg kell felelniük az *5.1. szakasz* követelményeinek.

4. **Tanúsítvány életciklus kezelés**

4.1. *A nemzet backendek regisztrálása*

A DCCG-rendszerben való részvételhez a tagállamoknak regisztrálniuk kell a DCCG-üzemeltetőnél. Ez a szakasz a nemzeti backend regisztrációja során követendő műszaki és operatív eljárást ismerteti.

A DCCG üzemeltetőjének és a tagállamnak információt kell cserélnie a bevezetési folyamat technikai kapcsolattartóiról. Vélelmezett, hogy a technikai kapcsolattartókat tagállamuk legitimálja, és az azonosítás/hitelesítés más csatornákon keresztül történik. A hitelesítés például akkor érhető el, ha egy tagállam műszaki kapcsolattartója az e-mailen keresztül jelszóval titkosított fájlként szolgáltatja a tanúsítványokat, és telefonon osztja meg a megfelelő jelszót a DCCG üzemeltetőjével. A DCCG-üzemeltető által meghatározott egyéb biztonságos csatornák is használhatók.

A tagállamnak három digitális tanúsítványt kell biztosítania a regisztrációs és azonosítási folyamat során:

— a tagállam NB_{TLS} TLS tanúsítványa,

— a tagállam NB_{UP} feltöltési tanúsítványa,

— a tagállam NB_{CSCA} CSCA tanúsítványa(i).

Valamennyi szolgáltatott tanúsítványnak meg kell felelnie az *5. szakaszban* meghatározott követelményeknek. A DCCG-üzemeltető ellenőrzi, hogy a szolgáltatott tanúsítvány megfelel-e az *5. szakaszban* foglalt követelményeknek. Az azonosítást és a regisztrálást követően a DCCG-üzemeltető:

— hozzáadja az NB_{CSCA} tanúsítványt/tanúsítványokat a $DCCG_{TA}$ nyilvános kulcsnak megfelelő titkos kulccsal aláírt bizalmi jegyzékhez,

— hozzáadja az NB_{TLS} tanúsítványt a DCCG TLS végpont engedélyezőlistájához,

— hozzáadja az NB_{UP} tanúsítványt a DCCG rendszerhez,

— átadja a tagállamok részére a $DCCG_{TA}$ és $DCCG_{TLS}$ nyilvánoskulcs-tanúsítványokat.

▼B

4.2. *Hitelesítésszolgáltatók, érvényességi idők és megújítás*

Abban az esetben, ha egy tagállam saját CSCA-t kíván működtetni, a CSCA-tanúsítványok önaláírt tanúsítványok is lehetnek. Ezek a tagállam bizalmi horgonyaként működnek, ezért a tagállamnak határozottan védenie kell a CSCA tanúsítvány nyilvános kulcsának megfelelő titkos kulcsot. Ajánlott, hogy a tagállamok egy offline rendszert használjanak CSCA-jukra, azaz olyan számítógépes rendszert, amely nem kapcsolódik egyetlen hálózathoz sem. A rendszerhez való hozzáféréshez többszemélyes ellenőrzést kell használni (például a négy szem elvét követve). A DSC-k aláírása után operatív ellenőrzéseket kell alkalmazni, és a titkos CSCA-kulcsot tároló rendszert biztonságosan kell tárolni, erős hozzáférés-ellenőrzésekkel. Biztonsági hardvermodulok vagy intelligens kártyák használhatók a CSCA titkos kulcsának további védelmére. A digitális tanúsítványok olyan érvényességi időszakot tartalmaznak, amely érvényesíti a tanúsítvány megújítását. Megújításra van szükség az új kriptográfiai kulcsok használatához és a kulcsméretek kiigazításához, ha a számításban alkalmazott új fejlesztések vagy új támadások veszélyeztetik az alkalmazott kriptográfiai algoritmus biztonságát. A héjmodellt kell alkalmazni (lásd a *3.2. szakaszt*).

Tekintettel a digitális Covid-igazolványok egyéves érvényességére, a következő érvényességi időtartamok ajánlottak:

— CSCA: 4 év,

— DSC: 2 év,

— feltöltés: 1–2 év,

— TLS ügyfélhitelesítés: 1–2 év.

Az időben történő megújításához a titkos kulcsokhoz a következő használati időszakok ajánlottak:

— CSCA: 1 év,

— DSC: 6 hónap.

A zökkenőmentes működés érdekében a tagállamoknak időben, például a lejárat előtt egy hónappal új feltöltési tanúsítványokat és TLS-tanúsítványokat kell létrehozniuk. A CSCA tanúsítványokat és a DSC-t legalább egy hónappal a titkos kulcs használatának lejárta előtt meg kell újítani (figyelembe véve a szükséges operatív eljárásokat). A tagállamoknak naprakész CSCA tanúsítványokat, feltöltési és TLS-tanúsítványokat kell benyújtaniuk a DCCG-üzemeltetőnek. A lejárt tanúsítványokat törölni kell az engedélyezőlistáról és a bizalmi jegyzékből.

A tagállamoknak és a DCCG-üzemeltetőnek nyomon kell követniük saját tanúsítványaik érvényességét. Nincs olyan központi szervezet, amely nyilvántartaná a tanúsítvány érvényességét és tájékoztatná a résztvevőket.

▼B

4.3. *A tanúsítványok visszavonása*

A digitális tanúsítványokat általában a kibocsátó hitelesítésszolgáltatójuk vonhatja vissza a tanúsítványvisszavonási listák vagy a valós idejű tanúsítvány-lekérdezés (OCSP) használatával. A DCC-rendszerhez tartozó CSCA-knak kell megadniuk a tanúsítványvisszavonási listákat (CRL-ek). Még ha ezeket a CRL-eket jelenleg nem is használják más tagállamok, azokat a jövőbeli alkalmazások érdekében integrálni kell. Amennyiben egy CSCA úgy dönt, hogy nem ad meg a CRL-eket, e CSCA DSC-it meg kell újítani, amikor a CRL-ek kötelezővé válnak. Az ellenőrzők nem használhatnak OCSP-t a DSC-k validálásához, és CRL-eket kell használniuk. Ajánlott, hogy a nemzeti backend végezze el a DCC-átjáróról letöltött DSC-k szükséges validálását, és csak megbízható és validált DSC-csomagot továbbítson a nemzeti DCC-validátoroknak. A DCC-validátorok a validálási folyamat során nem végezhetnek semmiféle visszavonás-ellenőrzést a DSC-n. Ennek egyik oka a DCC-birtokosok adatvédelme, elkerülve annak bármely lehetőségét, hogy egy adott DSC használatát a hozzá tartozó OCSP-válaszadó nyomon követhesse.

A tagállamok érvényes feltöltési és TLS-tanúsítványok használatával saját maguk törölhetik a DSC-iket a DCCG-ből. A DSC törlése azt jelenti, hogy az e DSC-vel kiadott valamennyi DCC érvénytelenné válik, amikor a tagállamok átadják a frissített DSC-listákat. A DSC-knek megfelelő titkos kulcsú anyagok védelme alapvető fontosságú. A tagállamoknak tájékoztatniuk kell a DCCG-üzemeltetőt, ha vissza kell vonniuk a feltöltési vagy TLS-tanúsítványokat, például a nemzeti backend sérülése miatt. A DCCG-üzemeltető ezt követően eltávolíthatja az érintett tanúsítvány megbízhatóságát, például azáltal, hogy törli azt a TLS engedélyezőlistáról. A DCCG-üzemeltető eltávolíthatja a tanúsítványok feltöltését a DCCG adatbázisból. Az e feltöltési tanúsítványnak megfelelő titkos kulccsal aláírt csomagok érvénytelenné válnak, ha a nemzeti backendek megszüntetik a visszavont feltöltési tanúsítvány megbízhatóságát. Amennyiben egy CSCA tanúsítványt vissza kell vonni, a tagállamok erről tájékoztatják a DCCG-üzemeltetőt és azon többi tagállamot, amellyel bizalmi kapcsolatban állnak. A DCCG-üzemeltető új bizalmi jegyzéket bocsát ki, amelyben az érintett tanúsítvány már nem szerepel. Az e CSCA által kiadott valamennyi DSC érvénytelenné válik, amikor a tagállamok frissítik a nemzeti backend bizalmi tárolójukat. Abban az esetben, ha a $DCCG_{TLS}$ tanúsítványt vagy a $DCCG_{TA}$ tanúsítványt vissza kell vonni, a DCCG üzemeltetőjének és a tagállamoknak együtt kell működniük egy új megbízható TLS-kapcsolat- és bizalmi jegyzék létrehozása érdekében.

5. **Tanúsítványminták**

Ez a szakasz a tanúsítványmintákra vonatkozó kriptográfiai követelményeket és iránymutatásokat, valamint követelményeket határozza meg. A DCCG-tanúsítványok esetében ez a szakasz határozza meg a tanúsítványmintákat.

5.1. *Kriptográfiai előírások*

A kriptográfiai algoritmusokat és a TLS titkosítási eszközkészleteket a Német Szövetségi Információbiztonsági Hivatal (BSI) vagy a SOG-IS hatályos ajánlása alapján kell kiválasztani. Ezek az ajánlások, valamint a többi intézmény és a szabványügyi szervezet ajánlásai hasonlóak. Az ajánlások a TR 02102-1 és TR 02102-2 ([1]) technikai iránymutatásokban vagy a SOG-IS kölcsönösen elfogadott kriptográfiai mechanizmusaiban találhatók ([2]).

([1]) BSI – Technical Guidelines TR-02102 (bund.de).
([2]) SOG-IS – Supporting documents (sogis.eu).

▼B

5.1.1. A DSC-re vonatkozó előírások

Az *I. melléklet 3.2.2. szakaszában* meghatározott előírásokat alkalmazni kell. Ezért határozottan ajánlott, hogy a dokumentum aláírók használják az Elliptikus görbéken alapuló digitális aláírási algoritmust (ECDSA) a NIST-p-256-tal együtt (a FIPS PUB 186-4 D. függelékében meghatározottak szerint). Egyéb elliptikus görbék nem támogatottak. A DCC helykorlátozásai miatt a tagállamoknak nem szabad használniuk az RSA-PSS-t, még akkor sem, ha az visszalépési algoritmusként engedélyezett. Amennyiben a tagállamok RSA-PSS-t használnak, 2048 bites vagy legfeljebb 3072 bites modulus méretet kell használniuk. A DSC aláíráshoz a ≥ 256 bit kimeneti hosszúságú SHA-2-t kell kriptográfiai hashfüggvényként használni (lásd ISO/IEC 10118-3:2004 szabványt).

5.1.2. A TLS-, feltöltési és CSCA tanúsítványokra vonatkozó előírások

Az elektronikus tanúsítványok és kriptográfiai aláírások tekintetében a DCCG összefüggésében a kriptográfiai algoritmusokra és a kulcshosszra vonatkozó főbb követelményeket az alábbi táblázat foglalja össze (2021-től):

Aláírás algoritmus	Kulcsméret	Hashfüggvény
EC-DSA	Legalább 250 bit	SHA-2 ≥ 256 bit kimeneti hosszúsággal
RSA-PSS (ajánlott kitöltés) RSA-PKCS#1 v1.5 (örökölt kitöltés)	Legalább 3000 bit RSA Modulus (N) e > 2^16 nyilvános kitevővel	SHA-2 ≥ 256 bit kimeneti hosszúsággal
DSA	Legalább 3000 bit prím p, 250 bit kulcs q	SHA-2 ≥ 256 bit kimeneti hosszúsággal

Az EC-DSA ajánlott elliptikus görbéje a széles körű végrehajtása miatt NIST-p-256.

5.2. *CSCA-tanúsítvány (NB_{CSCA})*

Az alábbi táblázat útmutatást nyújt az NB_{CSCA} tanúsítványmintájához, ha egy tagállam úgy dönt, hogy a DCC-rendszerhez saját CSCA-t működtet.

Félkövér betűtípust kell megadni (a tanúsítványban fel kell tüntetni), a *dőlt* betűtípus ajánlott (fel kell tüntetni). A hiányzó mezők esetében nem határoztak meg ajánlásokat.

Mező	Érték
Tárgy	**cn = <nem üres és egyedi közös név>**, *o = <Szolgáltató>,***c = <a CSCA-t működtető tagállam>**
Kulcshasználat	**Tanúsítvány aláírás,***CRL aláírás* (legalább)
Alapvető típusmegkötések	**CA = igaz, úthossz megkötések = 0**

A tárgynévnek nem üresnek és a meghatározott tagállamon belül egyedinek kell lennie. A (c) országkódnak egyeznie kell azzal a tagállammal, amely ezt a CSCA tanúsítványt fogja használni. A tanúsítványnak tartalmaznia kell az RFC 5280 ([1]) szabvány szerinti egyedi tárgykulcs-azonosítót (SKI).

([1]) rfc5280 (ietf.org).

▼B

5.3. *Dokumentum-aláíró tanúsítvány (DSC)*

Az alábbi táblázat iránymutatást nyújt a DSC-re vonatkozóan. **Félkövér** betűtípust kell megadni (a tanúsítványban fel kell tüntetni), a *dőlt* betűtípus ajánlott (fel kell tüntetni). A hiányzó mezők esetében nem határoztak meg ajánlásokat.

Mező	Érték
Sorozatszám	**egyedi sorozatszám**
Tárgy	**cn = <nem üres és egyedi közös név>**, *o = <Szolgáltató>*,**c = <ezt a DSC-t használó tagállam>**
Kulcshasználat	**digitális aláírás** (legalább)

A DSC-t a tagállam által használt CSCA-tanúsítványnak megfelelő titkos kulccsal kell aláírni.

A következő kiterjesztéseket kell használni:

— a tanúsítványnak tartalmaznia kell egy hatósági kulcsazonosítót (AKI), amely megfelel a kibocsátó CSCA-tanúsítvány tárgykulcs-azonosítójának (SKI);

— a tanúsítványnak tartalmaznia kell az RFC 5280 ([1]) szabvány szerinti egyedi tárgykulcs-azonosítót.

Ezenkívül a tanúsítványnak tartalmaznia kell a CRL elosztási pont kiterjesztését, amely a tanúsítványvisszavonási listára (CRL) utal, amelyet a DSC-t kibocsátó CSCA szolgáltat.

A DSC tartalmazhat egy kiterjesztett kulcshasználat-kiterjesztést nulla vagy annál több kulcshasználati szakpolitikai azonosítóval, amelyek korlátozzák azon HCERT-ek típusait, amelyeket ezzel a tanúsítvánnyal ellenőrizni lehet. Ha egy vagy több ilyen van, az ellenőrzők kötelesek ellenőrizni a kulcshasználatot a tárolt HCERT-tel összevetve. Ehhez a következő kiterjesztett kulcshasználati értékeket határozták meg:

Mező	Érték
kiterjesztett kulcshasználat	1.3.6.1.4.1.1847. 2021.1.1. tesztkibocsátók számára
kiterjesztett kulcshasználat	1.3.6.1.4.1.1847.2021.1.2. oltási kibocsátók számára
kiterjesztett kulcshasználat	1.3.6.1.4.1.1847.2021.1.3. gyógyulási kibocsátók számára

A kulcshasználat bármilyen kiterjesztésének hiányában (azaz nincs kiterjesztés vagy zéró kiterjesztés), ez a tanúsítvány bármely típusú HCERT validálására használható. Más dokumentumok meghatározhatják a HCERT-ek validálásához használt további releváns kibővített kulcshasználati szakpolitikai azonosítókat.

5.4. *Feltöltési tanúsítványok (NBUP)*

Az alábbi táblázat iránymutatást nyújt a nemzeti backend feltöltési tanúsítványra vonatkozóan. **Félkövér** betűtípust kell megadni (a tanúsítványban fel kell tüntetni), a *dőlt* betűtípus ajánlott (fel kell tüntetni). A hiányzó mezők esetében nem határoztak meg ajánlásokat.

([1]) rfc5280 (ietf.org).

▼B

Mező	Érték
Tárgy	**cn = <nem üres és egyedi közös név>**, *o = <Szolgáltató>*,**c = <ezt a feltöltési tanúsítványt használó tagállam>**
Kulcshasználat	**digitális aláírás** (legalább)

5.5. *Nemzeti backend TLS ügyfélhitelesítés (NB_{TLS})*

Az alábbi táblázat iránymutatást nyújt a nemzeti backend TLS ügyfélhitelesítési tanúsítványra vonatkozóan. **Félkövér** betűtípust kell megadni (a tanúsítványban fel kell tüntetni), a *dőlt* betűtípus ajánlott (fel kell tüntetni). A hiányzó mezők esetében nem határoztak meg ajánlásokat.

Mező	Érték
Tárgy	**cn = <nem üres és egyedi közös név>**, *o = <Szolgáltató>*,**c = <az NB-n található tagállam>**
Kulcshasználat	**digitális aláírás** (legalább)
Kibővített kulcshasználat	ügyfélhitelesítés (1.3.6.1.5.5.7.3.2)

A tanúsítvány tartalmazhat kiterjesztett kulcshasználati *szerver-hitelesítést (1.3.6.1.5.5.7.3.1) is*, de ez nem előírás.

5.6. *Bizalmi lista aláírási tanúsítvány ($DCCG_{TA}$)*

A következő táblázat a DCCG bizalmi horgony tanúsítványát határozza meg.

Mező	Érték
Tárgy	**cn = digitális zöldigazolvány átjáró** [1]**, o = <Szolgáltató>, c = <ország>**
Kulcshasználat	**digitális aláírás** (legalább)

5.7. *DCCG TLS szervertanúsítványok ($DCCG_{TLS}$)*

A következő táblázat a DCCG TLS tanúsítványt határozza meg.

Mező	Érték
Tárgy	cn = <FQDN vagy a DCCG IP-címe>, o = <Szolgáltató>, c = <ország>
Alany alt-név	dNS-név: <DCCG DNS név> vagy IP-cím: <DCCG IP-cím>
Kulcshasználat	**digitális aláírás** (legalább)
Kibővített kulcshasználat	szerver hitelesítés (1.3.6.1.5.5.7.3.1)

[1] Ebben az összefüggésben megmaradt az „uniós digitális Covid-igazolvány” helyett a „digitális zöldigazolvány” terminológia, mivel ez az a terminológia, amelyet a kódban rögzítettek és bevezettek az igazolványban, mielőtt a társjogalkotók új terminológiáról döntöttek volna.

▼B

A tanúsítvány tartalmazhat kiterjesztett kulcshasználati *ügyfélhitelesítést (1.3.6.1.5.5.7.3.2)* is, de ez nem előírás.

A DCCG TLS-tanúsítványát egy megbízható nyilvános hitelesítésszolgáltató bocsátja ki (amelynek a CAB Forum alapkövetelményeinek megfelelően valamennyi nagyobb böngészőben és operációs rendszerben szerepelnie kell).

▼M1

V. MELLÉKLET

JAVASCRIPT OBJEKTUM JELÖLÉS (JSON) SÉMA

1. **Bevezetés**

Ez a melléklet meghatározza a JSON-séma formájában megjelenő uniós digitális Covid-igazolványok (EUDCC) technikai adatszerkezetét. A dokumentum konkrét utasításokat tartalmaz az egyes adatmezőkkel kapcsolatban.

2. **A JSON-séma helye és verziói**

Az EUDCC hiteles és hivatalos JSON-sémája a következő internetcímen érhető el: https://github.com/ehn-dcc-development/ehn-dcc-schema. Más helyek nem hitelesek, de felhasználhatók a soron következő felülvizsgálatok előkészítéséhez.

Alapértelmezés szerint az e mellékletben meghatározott és a jelenleg igazolványokat kiállító összes ország által támogatott jelenlegi verzió a megadott webcím alatt szerepel.

A soron következő verzió, amelyet a Readme-fájl részletesebben ismertet, és egy meghatározott időponttól kezdve valamennyi országnak támogatnia kell, a megadott webcím alatt verziómegjelöléssel szerepel.

▼M3

3. **Közös szerkezetek és általános követelmények**

Nem állítható ki uniós digitális Covid-igazolvány, ha a hiányzó információk miatt nem lehet helyesen kitölteni az összes adatmezőt ezen előírásnak megfelelően. **Ez nem értelmezhető úgy, mint amely érinti a tagállamok azon kötelezettségét, hogy uniós digitális Covid-igazolványokat állítsanak ki.**

Az információk valamennyi mezőben megadhatók az UTF-8 használatával kódolt teljes UNICODE 13.0 karakterkészlettel, kivéve, ha kifejezetten értékkészletekre vagy szűkebb karaktercsoportokra korlátozódnak.

A közös struktúra a következő:

„JSON”:{

„ver”:<verzióadatok>,

„nam”:{

<személynévre vonatkozó adatok>

},

„dob”:<születési idő>,

„v” or „t” or „r”:[

{<oltóanyagdózisra vagy tesztelésre vagy gyógyultságra vonatkozó információk, egy bejegyzés>}

]

}

Az egyes csoportokra és mezőkre vonatkozó részletes információk a következő szakaszokban találhatók.

Ha a szabályok értelmében a mezőt ki kell hagyni, ez azt jelenti, hogy a mezőt üresen kell hagyni, és sem nevet, sem értéket nem tartalmazhat.

▼M3

3.1. *Verzió*

A verzióra vonatkozó információkat meg kell adni. A verziókövetés a Semantic Versioning (semver: https://semver.org) szerint történik. Az előállítás során a hivatalosan kiadott (jelenlegi vagy a korábbi hivatalos kiadású) verziók egyikét kell használni. További részletekért lásd a JSON Schema location szakaszt.

Mezőazonosító	A mező megnevezése	Utasítások
ver	Séma verzió	Megegyezik az EUDCC előállításához használt sémaverzió azonosítójával. Példa: „ver”:„1.3.0”

3.2. *A személy neve és születési ideje*

A személy neve a személy teljes hivatalos neve, amely megfelel az úti okmányokon feltüntetett névnek. A struktúra azonosítója: *nam*. Pontosan 1 (egy) személy nevét kell megadni.

Mezőazonosító	A mező megnevezése	Utasítások
nam/fn	Vezetéknév (vezetéknevek)	A birtokos vezetékneve(i) Ha a birtokosnak nincs vezetékneve és van utóneve, a mezőt ki kell hagyni. Minden más esetben pontosan 1 (egy) nem üres mezőt kell megadni, amelyben minden vezetéknév szerepel. Több vezetéknév esetén ezeket szóközzel kell elválasztani. A kötőjeleket vagy hasonló karaktereket is tartalmazó összetett neveknek azonban változatlannak kell maradniuk. Példák: „fn”:„Musterfrau-Gößinger” „fn”:„Musterfrau-Gößinger Müller”
nam/fnt	Szabványos vezetéknév (vezetéknevek)	A birtokos vezetékneve(i) a birtokos géppel olvasható úti okmányaiban használt (például a 9303 ICAO dokumentum 3. részében meghatározott szabályok szerinti) egyezmény alkalmazásával átírva. Ha a birtokosnak nincs vezetékneve és van utóneve, a mezőt ki kell hagyni. Minden más esetben pontosan 1 (egy) nem üres mezőt kell megadni, amelyben kizárólag A-Z és < karakterek szerepelnek. Maximális hosszúság: 80 karakter (a 9303 ICAO előírásnak megfelelően). Példák: „fnt”:„MUSTERFRAU<GOESSINGER” „fnt”:„MUSTERFRAU<GOESSINGER<MUELLER”
nam/gn	Utónév (utónevek)	A birtokos utóneve(i), például keresztneve(i): Ha a birtokosnak nincs utóneve és van vezetékneve, a mezőt ki kell hagyni. Minden más esetben pontosan 1 (egy) nem üres mezőt kell megadni, amelyben minden utónév szerepel. Több utónév esetén ezeket szóközzel kell elválasztani. Példa: „gn”:„Isolde Erika”

▼M3

Mezőazonosító	A mező megnevezése	Utasítások
nam/gnt	Szabványos utónév (utónevek)	A birtokos utóneve(i) a birtokos géppel olvasható úti okmányaiban használt (például a 9303 ICAO dokumentum 3. részében meghatározott szabályok szerinti) egyezmény alkalmazásával átírva. Ha a birtokosnak nincs utóneve és van vezetékneve, a mezőt ki kell hagyni. Minden más esetben pontosan 1 (egy) nem üres mezőt kell megadni, amelyben kizárólag A-Z és < karakterek szerepelnek. Maximális hosszúság: 80 karakter. Példa: „gnt”:„ISOLDE<ERIKA”
dob	Születési idő	A DCC-birtokos születési ideje. Teljes vagy részleges dátum, időbeli korlátozás nélkül, az 1900-01-01 és a 2099-12-31 közötti tartományra korlátozva. Pontosan 1 (egy) nem üres mezőt kell megadni, ha a teljes vagy részleges születési idő ismert. Ha a születési idő még részben sem ismert, a mezőbe üres „” karakterláncot kell beírni. Ennek meg kell egyeznie az úti okmányokban szereplő információkkal. Ha rendelkezésre áll a születési időre vonatkozó adat, az ISO 8601 szabvány szerinti formátumok egyikét kell használni. Egyéb lehetőségek nem támogathatók. ÉÉÉÉ-HH-NN ÉÉÉÉ-HH ÉÉÉÉ (Az ellenőrző alkalmazás megjelenítheti a születési idő hiányzó részeit a géppel olvasható úti okmányokban használt XX egyezmény alkalmazásával, pl. 1990-XX-XX.) Példák: „dob”:„1979-04-14” „dob”:„1901-08” „dob”:„1939” „dob”:„”

3.3. *Az igazolvány típusa szerinti információkra vonatkozó csoportok*

A JSON-séma az igazolvány típusa szerinti információkat tartalmazó bejegyzések három csoportját támogatja. Minden EUDCC pontosan 1 (egy) csoportot tartalmaz. Üres csoportok nem megengedettek.

Részcsoport azonosítója	Csoport neve	Bejegyzések
v	Oltási csoport	Ha van ilyen, pontosan 1 (egy) bejegyzést kell tartalmaznia, amely pontosan 1 (egy) oltóanyagdózist (egy dózist) ír le.
t	Teszt csoport:	Ha van ilyen, pontosan 1 (egy) bejegyzést kell tartalmaznia, amely pontosan 1 (egy) teszteredményt ír le.
r	Gyógyultsági csoport	Ha van ilyen, pontosan 1 (egy) bejegyzést kell tartalmaznia, amely pontosan 1 (egy) gyógyultsági igazolást ír le.

▼M1

4. **Az igazolvány típusa szerinti információk**

4.1. *Oltási igazolvány*

Oltási csoport, ha van ilyen, pontosan 1 (egy) bejegyzést kell tartalmaznia, amely pontosan egy oltási eseményt (egy dózist) ír le. Az oltási csoport valamennyi eleme kötelező, az üres értékek nem támogatottak.

▼**M1**

Mezőazonosító	A mező megnevezése	Utasítások
v/tg	Célzott betegség vagy kórokozó: Covid19 (SARS-CoV vagy annak egyik variánsa)	Kódolt érték a készletből disease-agent-targeted.json. Ehhez az értékhez egyetlen bejegyzés tartozik: 840539006, amely a SNOMED CT (GPS) Covid19-re vonatkozó kód. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "tg": "840539006"
v/vp	Covid19-oltóanyag vagy profilaxis	A használt oltóanyag vagy profilaxis típusa Kódolt érték a készletből vaccine-prophylaxis.json. Az értékkészlet a DCC-átjáróról kerül elosztásra. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "vp": "1119349007" (SARS-CoV-2 mRNS oltóanyag)
v/mp	Covid19-oltóanyag-termék	Az oltás e konkrét dózisához használt gyógyszer. ►**M4** Kódolt érték a készletből vaccine-medicinal-product.json. Vagy klinikai vizsgálatra utaló és a II. melléklet 3. szakaszában meghatározott szabálynak megfelelő kódolt érték. ◄ Az értékkészlet a DCC-átjáróról kerül elosztásra. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "mp": "EU/1/20/1528" (Comirnaty)
v/ma	A Covid19-oltóanyag forgalombahozatali engedélyének jogosultja vagy az oltóanyag gyártója	A forgalombahozatali engedély jogosultja vagy a gyártó, ha a forgalombahozatali engedély jogosultja nincs jelen. ►**M4** Kódolt érték a készletből vaccine-mah-manf.json. Vagy klinikai vizsgálatra utaló és a II. melléklet 4. szakaszában meghatározott szabálynak megfelelő kódolt érték. ◄ Az értékkészlet a DCC-átjáróról kerül elosztásra. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "ma": ORG-100030215 (Biontech Manufacturing GmbH)
v/dn	A dózis sorszáma	Az ezen oltási esemény során adott dózis sorszáma (pozitív egész szám). 1 az első dózis esetében, 2 a második dózis esetében stb. A II. melléklet 5. szakasza további részletes szabályokat tartalmaz. Pontosan 1 (egy) nem üres mezőt kell megadni. Példák: "dn": "1" (első dózis) "dn": "2" (második dózis) "dn": "3" (harmadik dózis)
v/sd	A dózisok teljes száma	A vakcinázási sorozatban beadott dózisok teljes száma (pozitív egész szám). A II. melléklet 5. szakasza további részletes szabályokat tartalmaz. Pontosan 1 (egy) nem üres mezőt kell megadni. Példák: "sd": "1" (egy dózisból álló elsődleges oltási sorozat esetén) "sd": "2" (két dózisból álló elsődleges oltási sorozat vagy egy dózisból álló elsődleges oltási sorozatot követő kiegészítő dózis esetén) "sd": "3" (pl. két dózisból álló elsődleges oltási sorozatot követő kiegészítő dózis esetén)

▼M1

Mezőazonosító	A mező megnevezése	Utasítások
v/dt	Az oltás dátuma	A leírt dózis beadásának dátuma, ÉÉÉÉ-HH-NN formátumban (teljes dátum idő nélkül). Egyéb formátumok nem támogathatók. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "dt": "2021-03-28"
v/co	Az a tagállam vagy harmadik ország, amelyben az oltást beadták	Az országot kétbetűs ISO3166 kód (AJÁNLOTT) vagy az oltási eseményért felelős nemzetközi szervezetre (például az UNHCR-re vagy a WHO-ra) való hivatkozás jelöli. Kódolt érték a készletből country-2-codes.json. Az értékkészlet a DCC-átjáróról kerül elosztásra. Pontosan 1 (egy) mezőt kell megadni. Példa: "co": "CZ" "co": "UNHCR"
v/is	Az igazolvány kiállítója	Az igazolványt kiállító szervezet neve. Az azonosítók a név részeként megengedettek, de a név nélkül szövegként történő önálló használatuk nem ajánlott. Legfeljebb 80 UTF-8 karakter. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "is": "Ministry of Health of the Czech Republic" "is": "Vaccination Centre South District 3"
v/ci	Egyedi igazolványazonosító	Egyedi igazolványazonosító (UVCI) az alábbi internetes oldalon meghatározottak szerint: https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf Az ellenőrző összeg beillesztése nem kötelező. A szöveg kiegészíthető az "URN:UVCI:" előtaggal. Pontosan 1 (egy) nem üres mezőt kell megadni. Példák: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.2. *Tesztigazolvány*

Teszt csoport, ha van ilyen, pontosan 1 (egy) bejegyzést kell tartalmaznia, amely pontosan egy teszteredményt ír le.

Mezőazonosító	A mező megnevezése	Utasítások
t/tg	Célzott betegség vagy kórokozó: Covid19 (SARS-CoV vagy annak egyik variánsa)	Kódolt érték a készletből disease-agent-targeted.json. Ehhez az értékhez egyetlen bejegyzés tartozik: 840539006, amely a SNOMED CT (GPS) Covid19-re vonatkozó kód. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "tg": "840539006"
t/tt	A teszt típusa	A használt teszt típusa a teszt tárgyát képező anyag alapján. Kódolt érték a készletből test-type.json (LOINC alapján). Az értékkészleten kívüli értékek nem megengedettek. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "tt": LP6464-4 (Nukleinsav-amplifikációs teszt szondával történő detektálással) "tt": LP217198-3 (Gyors immunvizsgálat)

▼M1

Mezőazonosító	A mező megnevezése	Utasítások
t/nm	A teszt neve (csak nukleinsav-amplifikációs tesztek esetében)	A használt nukleinsav-amplifikációs teszt (NAAT) neve. A névnek tartalmaznia kell a teszt gyártójának nevét és a teszt kereskedelmi megnevezését, vesszővel elválasztva. A NAAT-teszt esetében: a mező opcionális. ►M4 Antigén teszt esetében: a mező nem használható, mivel a teszt nevét közvetetten, a teszteszköz azonosítója segítségével adják meg (t/ma). ◄ Ha megadják a nevet, a mezőt nem szabad üresen hagyni. Példa: "nm": "ELITechGroup, SARS-CoV-2 ELITe MGB® Kit"

▼M4

t/ma	Teszteszköz azonosító (kizárólag antigén tesztek esetében)	Antigén teszt eszközazonosítója a JRC adatbázisából. Eszközkészlet (a HSC közös listája): — Valamennyi antigén teszt megtalálható a HSC közös listáján (ember által olvasható formában). — https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat (géppel olvasható, az értékkészletet alkotó listán szereplő id_device mező értékei) Az EU/EGT-országokban a kibocsátók csak a jelenleg érvényes értékhez tartozó tesztekre adhatnak ki igazolványokat. Az értékkészletet 24 óránként frissíteni kell. A harmadik országok által kiállított igazolványban az értékkészleten kívüli értékek is használhatók, az azonosítóknak azonban ekkor is a JRC adatbázisából kell származniuk. Más, például a tesztet végző gyártók által közvetlenül megadott azonosítók használata nem megengedett. Az ellenőrzők észlelik azokat az értékeket, amelyek nem tartoznak a naprakész értékkészlethez, és az ezeket tartalmazó igazolványokat érvénytelenként jelenítik meg. Ha egy azonosítót eltávolítanak az értékkészletből, az azt tartalmazó igazolványok az eltávolítás időpontjától számított legfeljebb 72 órán keresztül fogadhatók el. Az értékkészlet a DCC-átjáróról kerül elosztásra. Antigén teszt esetében: pontosan 1 (egy) nem üres mezőt kell megadni. A NAAT-teszt esetében: a mező nem használható, még akkor sem, ha a NAA tesztazonosító elérhető a JRC adatbázisában. Példa: „ma”: „344” (SD BIOSENSOR Inc, STANDARD F COVID-19 Ag FIA)

▼M1

t/sc	A mintavétel dátuma és időpontja	Az a dátum és időpont, amikor a tesztmintát gyűjtötték. Az időpont az időzónára vonatkozó információkat is tartalmazza. Az érték nem azt az időpontot jelöli, amikor a teszteredmény elkészült. Pontosan 1 (egy) nem üres mezőt kell megadni. Az ISO 8601 szabvány szerinti formátumok egyikét kell használni. Egyéb lehetőségek nem támogathatók. ÉÉÉÉ-HH-NNTóó:pp:mpZ ÉÉÉÉ-HH-NNTóó:pp:mp[+-]óó

▼M1

Mezőazonosító	A mező megnevezése	Utasítások
		ÉÉÉÉ-HH-NNTóó:pp:mp[+-]óópp ÉÉÉÉ-HH-NN óó:pp:mp[+-]óó:pp Példák: "sc": "2021-08-20T10:03:12Z" (UTC-idő) "sc": "2021-08-20T12:03:12+02" (CEST-idő) "sc": "2021-08-20T12:03:12+0200" (CEST-idő) "sc": "2021-08-20T12:03:12+02:00" (CEST-idő)
t/tr	Teszteredmény	A teszt eredménye. Kódolt érték a készletből test-result.json (a SNOMED CT, GPS alapján). Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "tr": "260415000" (Nem kimutatott)
t/tc	Tesztközpont vagy létesítmény	A tesztet végző szereplő neve. Az azonosítók a név részeként megengedettek, de a név nélkül szövegként történő önálló használatuk nem ajánlott. Legfeljebb 80 UTF-8 karakter. Minden további karaktert meg kell csonkítani. A név nem automatikus ellenőrzésre szolgál. A NAAT-tesztek esetében: pontosan 1 (egy) nem üres mezőt kell megadni. ►M4 Antigén teszt esetében: a mező opcionális. Ha megadják, nem maradhat üresen. ◄ Példa: "tc": "Test centre west region 245"
t/co	Az a tagállam vagy harmadik ország, amelyben a tesztet elvégezték	Az országot kétbetűs ISO3166 kód (AJÁNLOTT) vagy a teszt elvégzéséért felelős nemzetközi szervezetre (például az UNHCR-re vagy a WHO-ra) való hivatkozás jelöli. Kódolt érték a készletből country-2-codes.json. Az értékkészlet a DCC-átjáróról kerül elosztásra. Pontosan 1 (egy) mezőt kell megadni. Példák: "co": "CZ" "co": "UNHCR"
t/is	Az igazolvány kiállítója	Az igazolványt kiállító szervezet neve. Az azonosítók a név részeként megengedettek, de a név nélkül szövegként történő önálló használatuk nem ajánlott. Legfeljebb 80 UTF-8 karakter. Pontosan 1 (egy) nem üres mezőt kell megadni. Példák: "is": "Ministry of Health of the Czech Republic" "is": "North-West region health authority"

▼M1

Mezőazonosító	A mező megnevezése	Utasítások
t/ci	Egyedi igazolványazonosító	Az egyedi igazolványazonosító (UVCI) az alábbi internetes oldalon meghatározottak szerint: vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) Az ellenőrző összeg beillesztése nem kötelező. A szöveg kiegészíthető az "URN:UVCI:" előtaggal. Pontosan 1 (egy) nem üres mezőt kell megadni. Példák: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.3. *Gyógyultsági igazolvány*

Gyógyultsági csoport, ha van ilyen, pontosan 1 (egy) bejegyzést kell tartalmaznia, amely pontosan egy gyógyultsági igazolást ír le. A gyógyultsági csoport valamennyi eleme kötelező, az üres értékek nem támogatottak.

Mezőazonosító	A mező megnevezése	Utasítások
r/tg	A betegség vagy kórokozó, amelyből a birtokos felgyógyult: Covid19 (SARS-CoV-2 vagy annak egyik variánsa)	Kódolt érték a készletből disease-agent-targeted.json. Ehhez az értékhez egyetlen bejegyzés tartozik: 840539006, amely a SNOMED CT (GPS) Covid19-re vonatkozó kód. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "tg": "840539006"
r/fr	A birtokos első pozitív ►M4 ——— ◄-tesztje eredményének dátuma	Az a dátum, amikor a pozitív eredményt eredményező ►M4 ——— ◄-tesztmintát gyűjtötték ÉÉÉÉ-HH-NN formátumban (teljes dátum időpont nélkül). Egyéb formátumok nem támogathatók. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "fr": "2021-05-18"
r/co	Az a tagállam vagy harmadik ország, amelyben a tesztet elvégezték	Az országot kétbetűs ISO3166 kód (AJÁNLOTT) vagy a teszt elvégzéséért felelős nemzetközi szervezetre (például az UNHCR-re vagy a WHO-ra) való hivatkozás jelöli. Kódolt érték a készletből country-2-codes.json. Az értékkészlet a DCC-átjáróról kerül elosztásra. Pontosan 1 (egy) mezőt kell megadni. Példák: "co": "CZ" "co": "UNHCR"
r/is	Az igazolvány kiállítója	Az igazolványt kiállító szervezet neve. Az azonosítók a név részeként megengedettek, de a név nélkül szövegként történő önálló használatuk nem ajánlott. Legfeljebb 80 UTF-8 karakter. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "is": "Ministry of Health of the Czech Republic" "is": "Central University Hospital"

▼**M1**

Mezőazonosító	A mező megnevezése	Utasítások
r/df	Az igazolvány érvényességének kezdete	Az első dátum, amikortól az igazolványt érvényesnek kell tekinteni. A dátum nem lehet korábbi, mint az r/fr + 11 napként számított időpont. A dátumot ÉÉÉÉ-HH-NN formátumban kell megadni (teljes dátum időpont nélkül). Egyéb formátumok nem támogathatók. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "df": "2021-05-29"
r/du	Az igazolvány érvényességének vége	Az igazolvány kiállítója által megjelölt azon utolsó dátum, ameddig az igazolványt érvényesnek kell tekinteni. A dátum nem lehet későbbi, mint az r/fr + 180 napként számított időpont. A dátumot ÉÉÉÉ-HH-NN formátumban kell megadni (teljes dátum időpont nélkül). Egyéb formátumok nem támogathatók. Pontosan 1 (egy) nem üres mezőt kell megadni. Példa: "du": "2021-11-14"
r/ci	Egyedi igazolványazonosító	Az egyedi igazolványazonosító (UVCI) az alábbi internetes oldalon meghatározottak szerint: vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) Az ellenőrző összeg beillesztése nem kötelező. A szöveg kiegészíthető az "URN:UVCI:" előtaggal. Pontosan 1 (egy) nem üres mezőt kell megadni. Példák: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

▼M3

IV. MELLÉKLET

A TAGÁLLAMOKNAK MINT A VISSZAVONT UNIÓS DIGITÁLIS COVID-IGAZOLVÁNYOK JEGYZÉKEINEK CSERÉJÉRE SZOLGÁLÓ ÁTJÁRÓ KÖZÖS ADATKEZELŐINEK A FELELŐSSÉGI KÖRE

1. SZAKASZ

1. alszakasz

A felelősségi körök megosztása

(1) A közös adatkezelők az I. melléklet műszaki előírásainak megfelelően kezelik a bizalmi keretrendszer átjáróján keresztül továbbított személyes adatokat.

(2) A visszavonással – többek között az igazolvány visszavonásához vezető eljárással – kapcsolatos információk átjárón kívül történő gyűjtése, felhasználása, közzététele és egyéb feldolgozása tekintetében a tagállamok kiállító hatóságai maradnak az egyedüli adatkezelők.

(3) Minden adatkezelő felelős azért, hogy a személyes adatoknak a bizalmi keretrendszer átjáróján történő kezelése az általános adatvédelmi rendelet 5., 24. és 26. cikkével összhangban történjen.

(4) Minden adatkezelő létrehoz egy kapcsolattartó pontot, és azt egy funkcionális postafiókkal látja el a közös adatkezelők közötti, valamint a közös adatkezelők és az adatfeldolgozó közötti kommunikáció biztosítására.

(5) Az (EU) 2021/953 rendelet 14. cikkében említett bizottság által létrehozott munkacsoport feladata, hogy döntsön a visszavonási jegyzékek cseréjével és a személyes adatok kezelésére irányuló közös adatkezeléssel összefüggő kérdésekben, valamint hogy segítse a Bizottságnak mint adatfeldolgozónak szóló összehangolt utasítások kidolgozását. Ez a munkacsoport irányítja a közös adatkezelők döntéshozatali eljárását, és az általa elfogadandó eljárási szabályzatot kell alkalmazni. Alapszabályként az, hogy a közös adatkezelők valamelyike nem vesz részt e munkacsoport olyan ülésén, amelyet annak összehívása előtt legalább hét (7) nappal írásban bejelentettek, hallgatólagos beleegyezést jelent a munkacsoport ülésén született eredmények tekintetében. A közös adatkezelők bármelyike összehívhatja a munkacsoport ülését.

(6) Az adatfeldolgozónak szóló utasításokat a közös adatkezelők valamely kapcsolattartó pontja küldi meg a többi közös adatkezelővel egyetértésben, a munkacsoport fenti (5) bekezdésben ismertetett döntéshozatali eljárásának megfelelően. A közös adatkezelő írásban küldi meg az utasításokat az adatfeldolgozó részére, és erről tájékoztatnia kell az összes többi közös adatkezelőt. Ha a szóban forgó kérdés van annyira időérzékeny, hogy ne lehessen összehívni a fenti (5) bekezdésben említett munkacsoport ülését, akkor utasítás ennek ellenére adható, de a munkacsoport visszavonhatja azt. Az utasítást írásban kell megadni, és erről az utasítás megküldésekor minden más közös adatkezelőt tájékoztatni kell.

(7) A fenti (5) bekezdés szerint létrehozott munkacsoport nem zárja ki, hogy a közös adatkezelők egyéni hatáskörüket gyakorolva az általános adatvédelmi rendelet 33. és 24. cikkével összhangban tájékoztassák az illetékes felügyeleti hatóságot. Az ilyen értesítéshez nem szükséges a többi közös adatkezelő hozzájárulása.

▼M3

(8) A bizalmi keretrendszer átjárójának alkalmazási körében a megosztott felhasználói személyes adatokhoz kizárólag a kijelölt nemzeti hatóságok vagy hivatalos szervek által felhatalmazott személyek férhetnek hozzá.

(9) Valamennyi kiállító hatóság nyilvántartást vezet a felelősségi körébe tartozó adatkezelési tevékenységekről. A közös adatkezelés feltüntethető a nyilvántartásban.

2. alszakasz

Az érintettek kéréseinek kezelésével és az érintettek tájékoztatásával kapcsolatos felelősségi körök és feladatok

1. A kiállító hatóság szerepében eljáró egyes adatkezelők – az általános adatvédelmi rendelet 14. cikkével összhangban – tájékoztatják azokat a természetes személyeket, akiknek az igazolványát visszavonták (a továbbiakban: az érintettek) egyrészt a visszavonás tényéről, másrészt személyes adataiknak az uniós átjárón a visszavonási jegyzékek cseréjének támogatása céljából történő kezeléséről, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne.

2. Az egyes adatkezelők kapcsolattartó pontként szolgálnak azon természetes személyek számára, akiknek az igazolványát visszavonták, és foglalkoznak az érintettek vagy képviselőik által jogaiknak az általános adatvédelmi rendelettel összhangban történő gyakorlása keretében benyújtott kérelmekkel. Amennyiben egy közös adatkezelőhöz egy másik közös adatkezelő által kiállított igazolványra vonatkozó kérelem érkezik az érintettől, közli az érintettel a felelős közös adatkezelő kilétét és elérhetőségét. Egy másik közös adatkezelő kérésére a közös adatkezelők segítik egymást az érintettek kérelmeinek kezelésében, és indokolatlan késedelem nélkül, de legkésőbb a segítségnyújtás iránti kérelem kézhezvételétől számított 1 hónapon belül választ adnak egymásnak. Amennyiben a kérelem harmadik ország által benyújtott adatra vonatkozik, a kérelmet fogadó adatkezelő feladata azt kezelni, és közli az érintettel a harmadik ország kiállító hatóságának nevét és elérhetőségét.

3. Az egyes adatkezelők az érintettek rendelkezésére bocsátják e melléklet tartalmát, beleértve az 1. és 2. pontban megállapított szabályokat is.

2. SZAKASZ

A biztonsági események – többek között az adatvédelmi incidensek – kezelése

(1) A közös adatkezelők segítik egymást a biztonsági események azonosításában és kezelésében, ideértve az adatvédelmi incidensek azon eseteit is, amelyek az uniós átjárón történő adatkezeléshez kapcsolódnak.

2. A közös adatkezelők különösen a következőkről értesítik egymást:

a) a bizalmi keretrendszer átjáróján kezelt személyes adatok rendelkezésre állását, bizalmas jellegét és/vagy sértetlenségét érintő esetleges vagy tényleges kockázatok;

b) adatvédelmi incidensek, az adatvédelmi incidens valószínűsíthető következményei, a természetes személyek jogait és szabadságait érintő kockázatok értékelése, valamint az adatvédelmi incidens kezelése és a természetes személyek jogait és szabadságait érintő kockázatok csökkentése érdekében hozott intézkedések;

▼M3

c) a bizalmi keretrendszer átjáróján végzett adatkezelési műveletek technikai és/vagy szervezési biztosítékainak megsértése.

3. A közös adatkezelők az általános adatvédelmi rendelet 33. és 34. cikkével összhangban vagy a Bizottság által küldött értesítést követően tájékoztatják a Bizottságot, az illetékes felügyeleti hatóságokat és szükség esetén az érintetteket a bizalmi keretrendszer átjáróján végzett adatkezelési műveletekkel kapcsolatos minden adatvédelmi incidensről.

4. Valamennyi kibocsátó hatóság megfelelő műszaki és szervezési intézkedéseket hajt végre, amelyek célja:

a) a közösen feldolgozott személyes adatok elérhetőségének, integritásának és bizalmas jellegének biztosítása és védelme;

b) a birtokában lévő személyes adatok jogosulatlan vagy jogellenes kezelése, elvesztése, felhasználása, felfedése, megszerzése vagy az azokhoz való hozzáférés elleni védelem;

c) annak biztosítása, hogy a személyes adatokhoz való hozzáférést a címzetteken vagy adatfeldolgozókon kívül más személy számára ne tegyék lehetővé vagy engedélyezzék.

3. SZAKASZ

Adatvédelmi hatásvizsgálat

(1) Ha egy adatkezelőnek az (EU) 2016/679 rendelet 35. és 36. cikkében meghatározott kötelezettségei teljesítése érdekében egy másik adatkezelőtől információra van szüksége, erre irányulóan kérelmet kell küldenie az 1. szakasz 1. alszakaszának 4. pontjában említett funkcionális postafiókba. A másik adatkezelő minden tőle telhetőt megtesz a szóban forgó információk rendelkezésre bocsátása érdekében.

▼M3

VII. MELLÉKLET

A BIZOTTSÁGNAK MINT A VISSZAVONT UNIÓS DIGITÁLIS COVID-IGAZOLVÁNYOK JEGYZÉKEINEK CSERÉJÉT TÁMOGATÓ ÁTJÁRÓ ADATFELDOLGOZÓJÁNAK A FELELŐSSÉGI KÖRE

A Bizottság feladatai:

(1) A tagállamok nevében egy olyan biztonságos és megbízható kommunikációs infrastruktúrát hoz létre és bocsát rendelkezésre, amely támogatja az uniós átjárón keresztül benyújtott visszavonási jegyzékek cseréjét.

(2) A bizalmi keretrendszer átjárójának adatfeldolgozójaként rá háruló, a tagállamokkal szemben fennálló kötelezettségek teljesítése érdekében a Bizottság harmadik feleket is megbízhat további adatfeldolgozóként; a Bizottság tájékoztatja a közös adatkezelőket az egyéb további adatfeldolgozók megbízásával vagy leváltásával kapcsolatos tervezett változtatásról, ezáltal lehetővé téve az adatkezelők számára, hogy közösen kifogást emeljenek az ilyen változtatásokkal szemben. A Bizottság gondoskodik arról, hogy az e határozatban foglalt adatvédelmi kötelezettségek az említett további adatfeldolgozókra is alkalmazandók legyenek.

(3) A Bizottság a személyes adatokat kizárólag az adatkezelők dokumentált utasításai alapján kezeli, kivéve, ha az adatok kezelésére uniós vagy tagállami jogszabály vonatkozik; ebben az esetben a Bizottság az adatfeldolgozás megkezdése előtt tájékoztatja a közös adatkezelőket az említett jogi előírásról, kivéve, ha a szóban forgó jogszabály fontos közérdekből tiltja az ilyen tájékoztatást.

A Bizottság által végzett adatkezelés a következőket foglalja magában:

a) a nemzeti backend szerverek nemzeti backendszerver-tanúsítványok alapján történő hitelesítése;

b) a határozat 5a. cikkének (3) bekezdésében említett, a nemzeti backend szerverek által feltöltött adatok fogadása egy olyan alkalmazásprogramozási felületen, amely lehetővé teszi a nemzeti backend szerverek számára a megfelelő adatok feltöltését;

c) az adatok tárolása az uniós átjárón;

d) az adatok rendelkezésre bocsátása a nemzeti backend szerverek általi letöltés céljából;

e) az adatok törlése azok lejárati napján vagy az azokat benyújtó adatkezelő utasítására;

f) minden fennmaradó adat törlése a szolgáltatásnyújtás végét követően, kivéve, ha uniós vagy tagállami jogszabály előírja a személyes adatok tárolását.

(4) Az uniós átjáró karbantartása érdekében a Bizottság meghoz minden korszerű szervezeti, fizikai és logikai jellegű biztonsági intézkedést. A Bizottság e célból:

a) kijelöl egy, az uniós átjáró biztonsági irányításáért felelős szervezetet, közli a közös adatkezelőkkel annak elérhetőségét, és biztosítja, hogy az képes legyen reagálni a biztonsági fenyegetésekre;

▼M3

b) felelősséget vállal az uniós átjáró biztonságáért, beleértve a biztonsági intézkedések tesztelésének, értékelésének és felmérésének rendszeres elvégzését;

c) biztosítja, hogy az uniós átjáróhoz hozzáféréssel rendelkező valamennyi személyre szerződéses, szakmai vagy jogszabályban előírt titoktartási kötelezettség vonatkozzon.

(5) A Bizottság minden szükséges biztonsági intézkedést megtesz annak érdekében, hogy a nemzeti backend szerverek zavartalan működése ne kerüljön veszélybe. E célból a Bizottság megalkotja a backend szervereknek az uniós átjáróra történő csatlakozásával kapcsolatos konkrét eljárásokat. Ezek az alábbiakat foglalják magukban:

a) kockázatértékelési eljárás a rendszert fenyegető potenciális veszélyek azonosítása és mértékük megbecslése érdekében;

b) ellenőrzési és felülvizsgálati eljárás a következők céljából:

i. a végrehajtott biztonsági intézkedések és az alkalmazandó biztonsági politika közötti megfelelés ellenőrzése;

ii. a rendszerfájlok, a biztonsági paraméterek és a megadott engedélyek megbízhatóságának rendszeres ellenőrzése;

iii. a biztonság megsértésének és a behatolásoknak az észlelése érdekében történő nyomon követés;

iv. módosítások végrehajtása a meglévő biztonsági hiányosságok csökkentése érdekében; valamint

v. azon feltételek meghatározása, amelyek mellett – többek között az adatkezelők kérésére – engedélyezni lehet a független ellenőrzések elvégzését és hozzá lehet járulni azokhoz, ideértve a biztonsági intézkedésekkel kapcsolatos ellenőrzéseket és felülvizsgálatokat is, az EUMSZ-hez csatolt, az Európai Unió kiváltságairól és mentességeiről szóló 7. jegyzőkönyvet tiszteletben tartó feltételek mellett;

c) az ellenőrzési eljárás módosítása annak érdekében, hogy a módosítás végrehajtása előtt dokumentálható és értékelhető legyen a változás hatása, és hogy a közös adatkezelők tájékoztatást kapjanak minden olyan változásról, amely hatással lehet az infrastruktúráikkal való kommunikációra és/vagy azok biztonságára;

d) karbantartási és javítási eljárások meghatározása a berendezések karbantartása és/vagy javítása esetén követendő szabályok és feltételek meghatározása céljából;

e) biztonsági incidensekre vonatkozó eljárás meghatározása a jelentési és eszkalációs rendszer meghatározására, az érintett adatkezelők késedelem nélküli tájékoztatása, az adatkezelők késedelem nélküli tájékoztatása, hogy értesíthessék a nemzeti adatvédelmi felügyeleti hatóságokat minden adatvédelmi incidensről, valamint a biztonság megsértése esetén fegyelmi eljárás meghatározása;

(6) A Bizottság a technika állásának megfelelő fizikai és/vagy logikai biztonsági intézkedéseket hoz az uniós átjáró berendezéseinek otthont adó létesítmények számára, valamint a logikai adatok és a biztonsági hozzáférés ellenőrzése tekintetében. A Bizottság e célból:

a) érvényre juttatja a fizikai biztonságot a különleges biztonsági övezetek kialakítása és a jogsértések felderítése érdekében;

▼M3

b) ellenőrzi a létesítményekhez való hozzáférést, és nyomon követés céljából nyilvántartást vezet a látogatókról;

c) biztosítja, hogy az épületekbe való belépési engedéllyel rendelkező külső személyeket megfelelő felhatalmazással rendelkező személyzet kísérje;

d) biztosítja, hogy a kijelölt felelős szervek előzetes engedélye nélkül ne kerülhessen sor berendezések bevitelére, cseréjére vagy eltávolítására;

e) ellenőrzi a nemzeti backend szerverek és a bizalmi keretrendszer átjárójának egymáshoz való hozzáférését;

f) biztosítja az uniós átjáróhoz hozzáféréssel rendelkező személyek azonosítását és hitelesítését;

g) felülvizsgálja az uniós átjáróhoz való hozzáféréssel kapcsolatos engedélyezési jogokat abban az esetben, ha az infrastruktúra biztonsága sérül;

h) megőrzi az uniós átjárón keresztül továbbított információk sértetlenségét;

i) technikai és szervezési biztonsági intézkedéseket vezet be a személyes adatokhoz való jogosulatlan hozzáférés megakadályozására;

j) szükség esetén olyan intézkedéseket hajt végre, amelyek lehetővé teszik az uniós átjáróhoz való, a nemzeti hatóságok domainjéről kiinduló jogosulatlan hozzáférések megakadályozását (pl. helyszín/IP-cím blokkolása).

(7) A minőség és a biztonság alapelveitől és fogalmaitól való lényeges eltérés esetén a Bizottság lépéseket tesz a domain védelme érdekében, ideértve a kapcsolatok megszakítását is.

(8) A felelősségi körével kapcsolatban kockázatkezelési tervet tart fenn.

(9) Figyelemmel kíséri – valós időben – a bizalmi keretrendszer átjárója valamennyi szolgáltatási elemének teljesítményét, rendszeres statisztikákat készít és nyilvántartást vezet.

(10) Napi 24 órában telefonon, e-mailben vagy egy webportálon keresztül angol nyelven támogatást nyújt a bizalmi keretrendszer átjárójának valamennyi szolgáltatásához, és fogadja az engedélyezett hívó felek – az uniós átjáró koordinátorai és azok ügyfélszolgálatai, a projektfelelősök és a Bizottság által kijelölt személyek – hívásait.

(11) A Bizottság – amennyiben ez az (EU) 2018/1725 rendelet 12. cikkével összhangban lehetséges – megfelelő technikai és szervezési intézkedésekkel támogatást nyújt a közös adatkezelőknek azon kötelezettségük teljesítéséhez, hogy válaszoljanak az érintettek jogainak gyakorlásával kapcsolatos kérelmekre, mely jogokat az általános adatvédelmi rendelet III. fejezete határozza meg.

▼**M3**

(12) Az általános adatvédelmi rendelet 32., 33., 34., 35. és 36. cikke szerinti kötelezettségek teljesítése érdekében a Bizottság az uniós átjáróra vonatkozó információk megadásával támogatja a közös adatkezelőket.

(13) A Bizottság gondoskodik arról, hogy az uniós átjárón kezelt adatok minden, hozzáférési jogosultsággal nem rendelkező személy számára értelmezhetetlenek legyenek.

(14) A Bizottság minden szükséges intézkedést megtesz annak megakadályozására, hogy az uniós átjáró működtetői jogosulatlanul hozzáférhessenek a továbbított adatokhoz.

(15) A Bizottság intézkedéseket hoz, hogy elősegítse az uniós átjáró kijelölt adatkezelői közötti interoperabilitást és kommunikációt.

(16) A Bizottság az (EU) 2018/1725 rendelet 31. cikke (2) bekezdésének megfelelően nyilvántartást vezet a közös adatkezelők nevében végzett adatkezelési tevékenységekről.