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)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel 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 szóló (EU) 2021/953 európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 9. cikke (1) és (3) bekezdésére,

mivel:

(1) Az (EU) 2021/953 rendelet rendelkezik az uniós digitális Covid-igazolványról, aminek annak bizonyítását kell szolgálnia, hogy az adott személy megkapta a Covid19-oltóanyagot, a tesztje negatív eredményt mutatott vagy meggyógyult a fertőzésből.

(2) Annak érdekében, hogy az uniós digitális Covid-igazolvány az egész unióban működőképes legyen, technikai előírásokat és szabályokat kell meghatározni a digitális Covid-igazolványok kitöltése, biztonságos kiállítása és ellenőrzése, a személyes adatok védelmének biztosítása, az egyedi igazolványazonosító közös szerkezetének meghatározása, és az érvényes, biztonságos és interoperábilis vonalkód kibocsátása érdekében. Ez a bizalmi keretrendszer emellett meghatározza a nemzetközi szabványokkal és technológiai rendszerekkel való interoperabilitás biztosítását célzó feltételeket, és mint ilyen, modellként szolgálhat a világszintű együttműködéshez.

(3) Az uniós digitális Covid-igazolvány olvasása és értelmezése szükségessé teszi a közös adatstruktúrát és a hasznos adatok egyes adatmezőihez rendelt jelentésre és annak lehetséges értékeire vonatkozó megállapodást. Az ilyen interoperabilitás előmozdítása érdekében egy közös összehangolt adatstruktúrát kell meghatározni az uniós digitális Covid-igazolvány keretrendszeréhez. Az erre a keretre vonatkozó iránymutatásokat a 2011/24/EU európai parlamenti és tanácsi irányelv ([2]) alapján létrehozott e-egészségügyi hálózat alakította ki. Ezeket az iránymutatásokat figyelembe kell venni az uniós digitális Covid-igazolvány formáját és bizalmi kezelését meghatározó technikai előírások kialakítása során. Meg kell határozni az adatstruktúra leírását és a kódolási mechanizmusokat, továbbá egy olyan, géppel olvasható továbbítási kódolási mechanizmust (QR), amely megjeleníthető egy mobil eszköz képernyőjén vagy egy papírra kinyomtatható.

(4) Az uniós digitális Covid-igazolvány formáját és bizalmi kezelését meghatározó technikai előírások mellett az igazolványok kitöltésére vonatkozó általános szabályokat is meg kell határozni az uniós digitális Covid-igazolvány tartalmát képező kódolt értékekhez történő felhasználás céljából. A Bizottságnak az e-egészségügyi hálózat vonatkozó tevékenységére építve rendszeresen frissítenie kell és közzé kell tennie az e szabályokat végrehajtó adatállományokat.

(5) Az (EU) 2021/953 rendeletnek megfelelően az uniós digitális Covid-igazolványt alkotó hiteles igazolványoknak egy egyedi igazolványazonosító révén egyedileg azonosíthatónak kell lenniük, figyelemmel arra, hogy az (EU) 2021/953 rendelet hatályának időtartama alatt az állampolgárok részére egynél több igazolványt is kibocsáthatnak. Az egyedi igazolványazonosítónak egy alfanumerikus karakterláncból kell állnia, és a tagállamoknak biztosítaniuk kell, hogy ne tartalmazzon olyan adatokat, amelyek összekapcsolják azt más dokumentumokkal vagy azonosítókkal, például útlevél- vagy személyazonosító igazolványszámokkal, annak érdekében, hogy megakadályozzák a birtokos azonosítását. Az igazolványazonosító egyediségének biztosítása érdekében meg kell határozni az egyedi igazolványazonosító közös struktúrájára vonatkozó technikai előírásokat és szabályokat.

([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.).

([2]) Az Európai Parlament és a Tanács 2011/24/EU irányelve (2011. március 9.) a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről (HL L 88., 2011.4.4., 45. o.).

(6) Az uniós digitális Covid-igazolványt alkotó igazolványok biztonsága, hitelessége, érvényessége és sértetlensége, valamint ezek megfelelése az uniós adatvédelmi jognak alapvető fontosságú ahhoz, hogy ezeket valamennyi tagállamban elfogadják. Ezek a célok az uniós digitális Covid-igazolványok megbízható és biztonságos kibocsátására és ellenőrzésére vonatkozó szabályokat és az ezek infrastruktúráját meghatározó bizalmi keretrendszer révén valósulnak meg. A bizalmi keretrendszernek többek között egy olyan nyilvános kulcsú infrastruktúrán kell alapulnia, amely a tagállamok egészségügyi hatóságaitól vagy más megbízható hatóságoktól az uniós digitális Covid-igazolványokat kiállító egyes szervezetekig tartó bizalmi lánccal rendelkezik. Ezért az egész EU-ra kiterjedő interoperabilitási rendszer biztosítása érdekében a Bizottság kiépített egy központi rendszert – az uniós digitális Covid-igazolvány átjáróját (a továbbiakban: átjáró) –, amely az ellenőrzéshez használt nyilvános kulcsokat tárolja. Amikor egy QR-kódot beolvasnak, a digitális aláírást a megfelelő nyilvános kulcs segítségével ellenőrzik, amelyet korábban ebben a központi átjáróban tároltak. A digitális aláírások felhasználhatók az adatok sértetlenségének és hitelességének biztosítására. A nyilvános kulcsú infrastruktúrák a nyilvános kulcsok tanúsítványkiadókhoz való kötésével teremtenek bizalmat. Az átjáróban a hitelesség érdekében több nyilvános kulcsú tanúsítványt használnak. A nyilvános kulcsú anyagokra vonatkozó adatok tagállamok közötti biztonságos cseréjének biztosítása és a széles körű interoperabilitás lehetővé tétele érdekében meg kell határozni az alkalmazható nyilvánoskulcs-tanúsítványokat, és rendelkezni kell azok létrehozásának módjáról.

(7) Ez a határozat lehetővé teszi az (EU) 2021/953 rendelet követelményeinek olyan módon történő megvalósítását, amely a személyes adatok feldolgozását az uniós digitális Covid-igazolvány működőképessé tételéhez szükséges mértékre csökkenti, és hozzájárul ahhoz, hogy a végső adatkezelők általi végrehajtás megvalósításánál fogva tiszteletben tartsa az adatvédelmet.

(8) Az (EU) 2021/953 rendelettel összhangban az igazolványok kiadásáért felelős hatóságok vagy más kijelölt szervek az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([3]) 4. cikkének (7) bekezdésében említett adatkezelőknek minősülnek a kibocsátási folyamat során a személyes adatok feldolgozásával kapcsolatos szerepükben. Attól függően, hogy a tagállamok hogyan szervezik meg a kibocsátási folyamatot, egy vagy több hatóság vagy kijelölt szerv, például regionális egészségügyi szolgálatok is szerepet kaphatnak. A szubszidiaritás elvével összhangban ebben a kérdésben a tagállamok választhatnak. Ezért a tagállamok vannak a legjobb helyzetben, hogy több hatóság vagy más kijelölt szerv esetén biztosítsák, hogy ezek felelősségi körei egyértelműen megoszlanak, függetlenül attól, hogy különálló vagy közös adatkezelőkről van-e szó (például a regionális egészségügyi szolgálatok közös betegportált hoznak létre az igazolványok kiállítására). Hasonlóképpen, az igazolványoknak a rendeltetési vagy tranzit tagállam illetékes hatóságai, illetve a Covid19-világjárvány idején a nemzeti jogszabályok által bizonyos népegészségügyi intézkedések végrehajtására kötelezett, határokon átnyúló személyszállítási szolgáltatók által végzett ellenőrzése tekintetében, ezeknek az ellenőröknek meg kell felelniük az adatvédelmi szabályok szerinti kötelezettségeiknek.

(9) Az uniós digitális Covid-igazolvány átjáróján keresztül nem történik személyesadat-kezelés, mivel az átjáró csak az aláíró hatóságok nyilvános kulcsait tartalmazza. Ezek a kulcsok az aláíró hatóságokra vonatkoznak, és nem teszik lehetővé sem közvetlenül, sem közvetve azon természetes személy újraazonosítását, akinek az igazolványt kiállították. Az átjáró kezelőjeként a Bizottság tehát sem adatkezelőnek, sem adatfeldolgozónak nem minősül.

(10) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([4]) 42. cikkének (1) bekezdésével összhangban a Bizottság konzultált az európai adatvédelmi biztossal, aki 2021. június 22-én véleményt nyilvánított.

(11) Tekintettel arra, hogy az (EU) 2021/953 rendelet 2021. július 1-jétől történő alkalmazásához műszaki előírásokra és szabályokra van szükség, indokolt e határozat azonnali alkalmazása.

(12) Ezért – tekintettel az uniós digitális Covid-igazolvány gyors végrehajtásának szükségességére – e határozatnak a kihirdetése napján hatályba kell lépnie,

([3]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

([4]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

ELFOGADTA EZT A HATÁROZATOT:

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.

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.

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

Kelt Brüsszelben, 2021. június 28-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

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

– 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

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

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

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 ([3])) 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.

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 ([4]) 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]) rfc8230 (ietf.org).
([4]) rfc8392 (ietf.org).

3.2.6. Kibocsátás időpontja

A Kibocsátás időpontja (iat) kérésnek egész számot tartalmazó NumericDate formátumú időbélyegzővel kell rendelkeznie (az RFC 8392 ([5]), 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 ([6])) objektum, amely tartalmazza az egészségügyi állapotra vonatkozó információt. Ugyanazon kérés alapján több különböző típusú egészségügyi igazolvány is létezhet, amelyek közül a DCC egy.

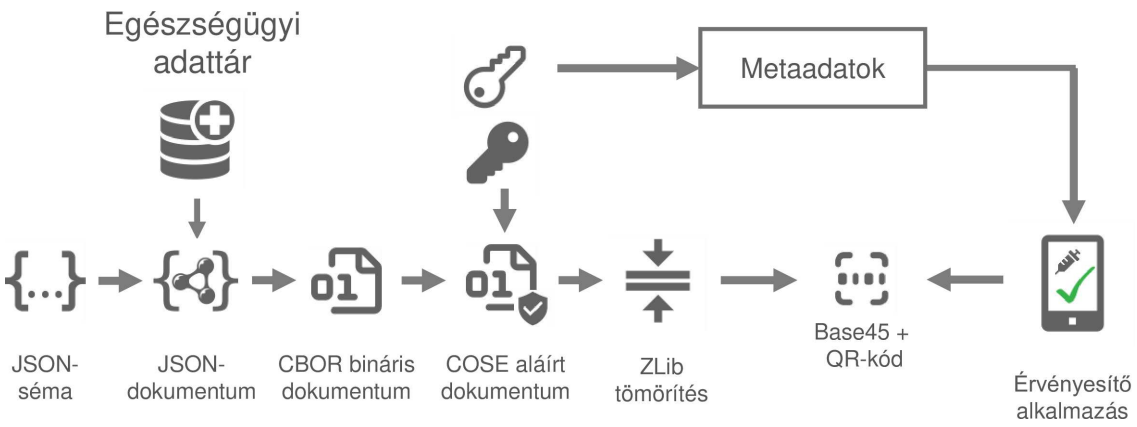
A JSON tisztán csak séma célokat szolgál. A reprezentációs formátum az RFC 7049 ([7]) szabványban meghatározott CBOR. Az alkalmazásfejlesztők valójában sohasem dekódolják vagy kódolják a JSON-formátumot, hanem a memóriában található szerkezetet használhatják.

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

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) 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.).

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.

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 ([9])) és az RFC 1951 ([10]) 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.

([9]) rfc1950 (ietf.org).
([10]) rfc1951 (ietf.org).

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.

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 ([11]) 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.

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.

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

II. MELLÉKLET

AZ UNIÓS DIGITÁLIS COVID-IGAZOLVÁNY KITÖLTÉSÉRE VONATKOZÓ SZABÁLYOK

Az e mellékletben meghatározott értékkészletekre vonatkozó általános szabályok célja a szemantikai szintű interoperabilitás biztosítása, és lehetővé teszik a DCC 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 ajánlott az UTF-8 kódolás (név, tesztközpont, igazolvány kibocsátója). A naptári dátumokat (születési idő, oltás időpontja, a tesztminta gyűjtésének időpontja, az első pozitív teszteredmény időpontja, az igazolvány érvényességének időpontjai) tartalmazó adatmezőket ajánlott az ISO 8601 szabvány szerint kódolni.

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.

Az értékkészleteket a Bizottság az e-egészségügyi hálózat és az Egészségügyi Biztonsági Bizottság támogatásával rendszeresen frissíti. 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)**

   Előnyben részesített kódrendszer: SNOMED CT.

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

   A kiválasztott kódoknak a Covid19-re vagy, amennyiben részletesebb információkra van szükség a SARS-CoV-2 genetikai változatára vonatkozóan, ezekre a változatokra kell vonatkozniuk, ha járványügyi okokból ilyen részletes információkra van szükség.

   A használandó kódra példa a 840539006 (Covid19) SNOMED CT kód.

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). Az értékkészletet ki kell bővíteni, ha új oltóanyagtípusokat fejlesztenek ki és alkalmaznak.

3. **Covid19-oltóanyag gyógyszer**

   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).

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).

5. **Több dózisból hányadik és a dózisok teljes száma**

Az 1. igazolványban használandó.

Két mező:

(1) az egy ciklusban alkalmazott dózisok száma;

(2) a teljes ciklusban várható dózisok száma (az alkalmazás időpontjában egy személyre jellemző).

Például az 1/1, 2/2 befejezettként jelenik meg; beleértve az 1/1 lehetőséget a két dózist tartalmazó vakcinák tekintetében, amelyek esetében azonban a tagállam által alkalmazott protokoll szerint egy dózist kell beadni azoknak, akiket az oltás előtt Covid19-cel diagnosztizáltak. A dózisok teljes számát a dózis beadásakor rendelkezésre álló információk szerint kell megadni. Ha például egy adott oltóanyag esetében a legutolsó beadott oltáskor egy harmadik oltást (booster) kell elvégezni, a második mezőszámnak ezt kell tükröznie (például 2/3, 3/3 stb.).

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.

7. **A teszt típusa**

Előnyben részesített kódrendszer: LOINC.

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 ebben az értékkészletben szereplő kódoknak a teszt módszerére kell vonatkozniuk, és azokat legalább a NAAT-teszteknek RAT-tesztektől való elhatárolásához kell kiválasztani, az (EU) 2021/953 rendeletben meghatározottak szerint.

Az előnyben részesített kódrendszerben használandó kódra példa az LP217198-3 (gyors immunvizsgálat).

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

Előnyben részesített kódrendszer: A HSC antigén gyorstesztek JRC által fenntartott jegyzéke (Covid19 *in vitro* diagnosztikai eszközök és tesztmódszerek adatbázisa).

A 2. igazolványban használandó.

Az értékkészletnek tartalmaznia kell a Covid19 antigén gyorsteszteknek a 2021/C 24/01 tanácsi ajánlás alapján létrehozott és az Egészségügyi Biztonsági Bizottság által jóváhagyott közös és aktualizált jegyzékében felsorolt antigén gyorstesztek 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.

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. **A teszt eredménye**

Előnyben részesített kódrendszer: SNOMED CT.

A 2. igazolványban használandó.

A kiválasztott kódoknak lehetővé kell tenniük a pozitív és a negatív (kimutatott vagy nem kimutatható) teszteredmények megkülönböztetését. Ha a felhasználási esetek ezt megkövetelik, további (pl. meghatározatlan) értékek adhatók hozzá.

Az előnyben részesített kódrendszerből használandó kódokra példák a 260415000 (nem kimutatható) és 260373001 (kimutatott).

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.

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]), ([2]) szabvány szerinti, elválasztásra szolgáló további különleges karakterekkel, azaz {„/”, „#”, „:”}.

(2) Maximális hosszúság: a tervezőknek 27–30 karakter hosszúságra kell törekedniük ([3]).

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

(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 tagállamoknak ellenőrző összeget kell használniuk, ha valószínűsíthető, hogy továbbítás, (emberi) átírás vagy egyéb sérülés következhet be (azaz a nyomtatásban történő használat esetén).

5.2. Az igazolvány validálásához nem szabad 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) ([4]) szabvány szerinti összefoglalójának kell lennie digitális/vezetékes továbbítási formátumban. Az ellenőrző összeget „#” karakter választja el az UCI többi részétől.

([1]) rfc3986 (ietf.org).

([2]) Az olyan mezők, mint a nem, a tétel/egység száma, az alkalmazó központ, az egészségügyi szakember azonosítása, a következő oltási időpont nem feltétlenül szükségesek orvosi felhasználástól eltérő célokra.

([3]) 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.

([4]) 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 (esetünk alfa karakterekkel) működjön.

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

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

Az e-egészségügyi hálózatnak az ellenőrizhető oltási igazolványokra és az alapvető interoperabilitási elemekre vonatkozó iránymutatásai ([5]) 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.

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

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
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

Kifejezés	Meghatározás
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.

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.

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.

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.

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.

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]).

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

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

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 ([3]) szabvány szerinti egyedi tárgykulcs-azonosítót (SKI).

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)

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

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 ([4]) 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.

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)

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

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** ([5])**, 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)

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).

([5]) 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.