



Brüsszel, 2026. július 10.
(OR. en)

11772/26
ADD 1

SOC 490
ANTIDISCRIM 73
FREMP 243
TRANS 497
SPORT 38
CULT 94
DELECT 110

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2026. július 1.
Címzett:	Thérèse BLANCHET, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	C(2026) 4534 annex
Tárgy:	MELLÉKLETEK a következőhöz: A BIZOTTSÁG (EU) .../... VÉGREHAJTÁSI RENDELETE az (EU) 2024/2841 irányelvnek az európai fogyatékosági kártya fizikai változatán található QR-kód meghatározása, valamint a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatán található QR-kód meghatározása és az annak biztonságát biztosító közös műszaki előírások megállapítása, valamint az interoperabilitással kapcsolatos kérdések tekintetében történő kiegészítéséről



Brüsszel, 2026.7.1.
C(2026) 4534 final

ANNEXES 1 to 4

MELLÉKLETEK

a következőhöz:

A BIZOTTSÁG (EU) .../... VÉGREHAJTÁSI RENDELETE

az (EU) 2024/2841 irányelvnek az európai fogyatékosági kártya fizikai változatán található QR-kód meghatározása, valamint a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatán található QR-kód meghatározása és az annak biztonságát biztosító közös műszaki előírások megállapítása, valamint az interoperabilitással kapcsolatos kérdések tekintetében történő kiegészítéséről

I. MELLÉKLET

AZ EURÓPAI FOGYATÉKOSSÁGI KÁRTYA FIZIKAI VÁLTOZATÁN TALÁLHATÓ QR-KÓDRA VONATKOZÓ ELŐÍRÁSOK

1. Az európai fogyatékosági kártya fizikai változatán található QR-kód formátuma

(a) **2. modell szerinti QR-kód formátum**, az ISO/IEC 18004:2024 vagy azzal egyenértékű nemzetközi QR-kód-specifikációknak megfelelően.

(b) **M hibajavítási szint** (15 %-os redundancia), amely biztosítja a nyomtatott QR-kód karcolásokkal vagy részleges károsodásával szembeni ellenálló képességet.

(c) **Kódolási mód:** A QR-kódban foglalt hasznos információ az issuerSigned tömör binárisobjektum-reprezentációs (CBOR) struktúra és a megfelelő issuerAuth COSE_Sign1 aláírási objektum kombinációjából áll, a CBOR-objektum aláírásban és titkosításban (a továbbiakban: COSE, RFC 9052 szabvány 3.1., 4.2. és 4.4. szakasz) meghatározottak szerint, amely az issuerSigned tételek esetében az mDOC adatmodellt követi, de hozzá van igazítva a statikus fizikai kártya használatához. Az issuerAuth egy COSE_Sign1 objektum, és egy x5t fejléc paramétert (a COSE X.509 tanúsítvány az RFC 9360 szabványban (2. szakasz) meghatározott hasítófüggvény fejléc paramétere) tartalmazó alg = ES256 algoritmus; az interoperabilitás érdekében az x5t fejléc paraméterben alkalmazott hash algoritmus az SHA-256.

(d) A QR-kód kódolása előtt a kombinált CBOR/COSE objektumot **zlib formátum alkalmazásával tömöríteni kell** (RFC 1950 szabvány, 2.2. szakasz) **a Deflate algoritmussal** (RFC 1951 szabvány, 3.2. és 4. szakasz). Az így kapott tömörített bájtömböt a **QR-kódban bájt módban** kell kódolni, biztosítva a bináris CBOR/COSE hasznos adatok és a szkener interoperabilitásának teljes körű támogatását.

A kibocsátóknak a QR-kódban foglalt hasznos adatokban szereplő valamennyi szövegmező esetében UTF-8 Unicode karaktereket kell kódolniuk a CBOR szövegsorokon belül. Az aláírt hasznos adatokra nem alkalmazható átírás. Az interoperabilitás érdekében a kibocsátóknak az aláírás előtt minden szöveges mezőben az Unicode C normalizációs formát (NFC) kell alkalmazniuk.

(e) **Előtag:** Az európai fogyatékosági kártyán található QR-kód karakterlánc az „ED1:MDOC:” kóddal kezdődik. Ez a kártyatípust és a kódolási profilt azonosítja. Az előtagoknak különbséget kell lenniük a kis- és nagybetűk között, és meg kell jelenniük. Az ismeretlen vagy nem támogatott előtagok elutasítást eredményeznek. Az előtagot és a tömörített hasznos adatokat egyetlen bájt mód adatszégmengként kell kódolni a QR-kódban.

(f) A **modul legkisebb mérete $\geq 0,25$ mm** a nyomtatott kártyák olvashatóságának biztosítása érdekében.

(g) **Maximális Verzió: 20;** mindkét oldalon legfeljebb 97×97 mm-s modullal.

2. Az európai fogyatékosági kártya aláírás-generálási előírásai

Az európai fogyatékosági kártyán található QR-kódok bélyegzésére használt minősített elektronikus bélyegző (QSeal) biztosítja, hogy a kódolt adatok az engedélyezett kibocsátó hatóságtól származnak, és azokat nem módosították.

- (a) **Aláírási algoritmus:** Az aláírási algoritmus az ES256 (Elliptikus görbéken alapuló digitális aláírási algoritmus (ECDSA) a P-256 görbét alkalmazó SHA-256 hash algoritmussal együtt), az RFC 9053 szabvány (2.1. szakasz) meghatározása szerint; a COSE-ben az algoritmust az RFC 9052 szabványban (3.1. szakasz) meghatározott algoritmikus fejléc-paraméterével azonosítják.
- (b) **Aláírási kulcs:** A QR-kódban foglalt hasznos adatokat az elektronikus bélyegző minősített tanúsítványának (QSealC) megfelelő titkos kulcs használatával kell aláírni.
- (c) **COSE-struktúra:** Az aláírás-konténernek a COSE_Sign1 objektumnak kell lennie. A védett fejlécnek az (ES256) algoritmust és az x5t fejléc paramétert (a COSE X.509 tanúsítvány RFC 9360 szabványban (2. szakasz) meghatározott hasítófüggvény fejléc paramétere) kell tartalmaznia; az interoperabilitás érdekében az x5t fejléc paraméterben alkalmazott hash algoritmus az SHA-256. A hitelesítés során az x5t értéket kell használni a megfelelő tanúsítvány keresésére a hitelesítőnek a megbízható szolgáltatók listájában szereplő információkból álló helyi bizalmi tárolójában, majd az eIDAS bizalmi keretrendszerrel összhangban hitelesíteni kell a tanúsítványláncot és a tanúsítvány státuszát.
- (d) **Aláírás Standard:** A QR-kódban foglalt hasznos adatokat COSE_Sign1 objektumként kell aláírni az RFC 9052 szabványnak (4. szakasz), a CBOR-objektumaláírásnak és titkosításnak megfelelően. A COSE_Sign1 objektumot az issuerAuth tárolja, és azt a COSE_Sign1-t jelölő CBOR-címke nélkül kell kódolni. A COSE_Sign1 objektum hasznos adatmezőjét le kell választani, és üres CBOR értéként kell kódolni. Az aláírás létrehozása és ellenőrzése esetében a külső hasznos adattartalom a determinisztikus kódolt CBOR-szerkezet, amely tartalmazza a felső szintű CBOR kulcs-érték párokban (map) szereplő docType értéket és issuerSigned értéket.
- (e) **Hash Algoritmus:** Az aláírások generálásához és az integritás ellenőrzéséhez az ES256 algoritmus részét képező SHA-256 hash algoritmust kell használni.
- (f) **Kódolás:** A hasznos adatokat a tömör binárisobjektum-reprezentáció (CBOR) (RFC 8949 szabvány, 4.2. szakasz) alkalmazásával kell kódolni, a COSE- és mDOC-előírásoknak megfelelően, biztosítva az aláírt adatok kódolását és reprodukálhatóságát.

3. Nyomtatási előírások

- (a) **Világos mező:** A QR-kód minden oldalán **4 modulból** álló világos mezőt kell hagyni, amelyen nem szerepel nyomtatás, minta vagy háttérszín.
- (b) **Kontraszt:** A QR-kódot fehér háttérre kell nyomtatni, legalább **4:1** kontrasztarány mellett, hogy változó világítási körülmények között is könnyen olvasható legyen.
- (c) A QR-kódot az (EU) 2024/2841 irányelv I. mellékletében meghatározott szín használatával kell nyomtatni, amely biztosítja a maximális kontrasztot.
- (d) **Elhelyezés és méret:** A QR-kódnak a világos mezővel együtt 26,25 mm × 26,25 mm méretűnek kell lennie és a kártya hátoldalán, a jobb alsó sarokban kell azt elhelyezni. A QR-kód legfeljebb a 20. verzióknak (97 × 97 modul) megfelelő lehet, 0,25 mm-es vagy annál nagyobb modulmérettel.

A QR-kódot a világos mezővel együtt a kártya jobb szélétől legalább 5 mm-re, és alsó szélétől legalább 5 mm-re kell elhelyezni.

4. Az európai fogyatékosági kártyán található QR-kódban szereplő adatok

A QR-kódnak tartalmaznia kell egy minimális, offline ellenőrizhető adatkészletet az (EU) 2016/679 rendelet 5. cikke (1) bekezdésének c) pontjában meghatározott adattakarékosság elvének megfelelően. A hasznos adatok struktúrája a következő:

- (a) A kártyaattribútumokat az issuerSigned objektumon belül kódolják a CBOR-ban.
- (b) A struktúrát a kibocsátó hatóság issuerAuth-ként (COSE_Sign1, x5t hash algoritmust tartalmazó ES256 algoritmus, a COSE X.509 tanúsítvány hash fejléc paramétere) minősített elektronikus bélyegzővel (QSeal) csomagolja be és írja alá.
- (c) A létrejövő CBOR/COSE objektumot e melléklet 1. d) pontjának megfelelően tömöríteni kell. A QR-kódban foglalt hasznos információ az „ED1:MDOC:” előtagból és az utána következő, létrejövő tömörített bájtömbből áll, és a teljes hasznos adattartalmat bájt módban, egyetlen QR-kód adatszégmengként kell kódolni.

Az adattartalom az (EU) 2024/2841 irányelv I. mellékletében felsorolt, a kártya előlapján található mezőkben szereplő látható adatok részhalmazából (családi név, utónév, a kártya sorozatszám, lejáratási idő), valamint a visszavonási azonosítóból, az elektronikus aláírásból és a sémainformációból áll.

Az **elektronikus aláírásnak** a következőket kell tartalmaznia:

- i. issuerAuth – A kibocsátó hatóság **QSealC titkos kulcsával** aláírt COSE_Sign1 objektum;
- ii. védett fejléc, amely tartalmazza az alg = ES256 (aláírási algoritmus) és x5t (a COSE X.509 tanúsítvány hash fejléc paramétere) értéket.

5. Opcionális adatok

A QR-kód nem tartalmazhat opcionális adatokat.

6. Visszavonási azonosító

A látható kártyasorozatszám mellett a QR-kódnak tartalmaznia kell egy külön visszavonási azonosítót.

A visszavonási azonosítót kell használni a visszavont státusz meghatározásához és a visszavonási jegyzék kezeléséhez. A visszavonási azonosító nem nyomtatható a kártyára, és nem jeleníthető meg a kártyaellenőrök számára.

6.1. A visszavonási azonosítóra vonatkozó követelmények

A visszavonási azonosítónak:

- (a) szerepelnie kell a QR-kódban foglalt, aláírt hasznos adatokban;
- (b) egyedinek kell lennie legalább a kibocsátó hatóság kibocsátási doménjén belül;
- (c) nem nyomtatható a kártyára, és nem lehet ember által olvasható;
- (d) ne fedhet fel személyes adatokat, és nem bírhat közvetlen jelentéssel;

- (e) nem származhat közvetlenül a látható kártyasorozatszámából; valamint
- (f) annak minősített elektronikus bélyegzővel kriptográfiailag összekapcsolva kell lennie a QR-kódban foglalt hasznos adatokkal.

6.2. *A visszavonási azonosító formátuma és mérete*

A visszavonási azonosítót CBOR bájt sorozatként (bstr) kell kódolni. A visszavonási azonosítónak 16 bájt (128 bit) hosszúságúnak kell lennie.

A visszavonási azonosítót a kibocsátó hatóság az ellenőrzése alatt álló módszerrel kell generálni, amely biztosítja a megfelelő információs entrópiát és a találgatással (guessing) vagy felsorolással (enumeration) szembeni rezisztenciát.

6.3. *Visszavonási jegyzékek*

Az ellenőrzési célból közzétett visszavonási jegyzékekben csak a visszavont kártyák visszavonási azonosítója szerepelhet. A kártya sorozatszámái nem tehetők közzé a visszavonási jegyzékekben.

7. **Az európai fogyatékosági kártyán található tömör binárisobjektum-reprezentációban (CBO) szereplő hasznos adatok (a QR-kódon belül)**

A QR-kódban foglalt hasznos adatokon belül csak a következő adatok tüntethetők fel, összhangban az európai fogyatékosági kártyának az (EU) 2024/2841 irányelv I. mellékletében meghatározott látható adatmezőivel:

Felső szintű tartalom:

- (a) docType = "eu.edc"
- (b) issuerSigned.nameSpaces."eu.edc" az alábbi táblázatban feltüntetett attribútumokkal
- (c) issuerAuth = COSE_Sign1 (QSeal)

Mező	mDOC path	Típus/Formátum
Adatséma verzió	issuerSigned.nameSpaces."eu.edc".ver	Karakterlánc (pl. „1.0”)
Kártya típusa: európai fogyatékosági kártya	docType	Enum ("eu.edc")
A kártya sorozatszáma	issuerSigned.nameSpaces."eu.edc".sub	Karakterlánc
Visszavonási azonosító	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bájt)
A kártyatulajdonos utóneve	issuerSigned.nameSpaces."eu.edc".givenName	Unicode szövegsor (UTF-8)

A kártyatulajdonos vezetékneve	issuerSigned.nameSpaces."eu.edc".familyName	Unicode szövegsor (UTF-8)
A kártya érvényessége	issuerSigned.nameSpaces."eu.edc".exp	az RFC 8943 szabványban (2.1. szakasz) meghatározott 1004 CBOR-címke, amely egy, az RFC 3339 szabványnak megfelelő, ÉÉÉ-HH-NN formátumú teljes dátumot reprezentáló UTF-8 szövegsort tartalmaz

Az elektronikus aláírást az issuerAuth (COSE_Sign1 objektum) tárolja. A tanúsítványlánc nem építhető be a QR-kód hasznos adattartalmába; ehelyett a védett COSE fejlécnek tartalmaznia kell az x5t tanúsítvány ujjlenyomat-algoritmust, amely arra szolgál, hogy a hitelesítő gyorsítótárazott bizalmi tárolójában megtalálható legyen a megfelelő QSealC-tanúsítvány.

8. Az európai fogyatékosági kártyán található QR-kódban foglalt hasznos adatok példája: JavaScript Objektum Jelölés stílusú kommentált logikai reprezentáció

A következő példa az európai fogyatékosági kártya logikai nézetének ember által olvasható JavaScript Objektum Jelölés (JSON) reprezentációja. A gyakorlatban ez a struktúra nem lehet ember által olvasható, mivel:

- (a) CBOR-ban van kódolva (RFC 8949 szabvány, 3. szakasz),
- b) jelölés nélküli COSE_Sign1 szerkezet alkalmazásával van aláírva, és a hasznos adattartalom le van választva (RFC 9052 szabvány, 4. szakasz),
- c) lejárat dátumot tartalmaz, amelyet az RFC 8943 szabvány (2.1. szakasz) szerinti, teljes dátum értéket tartalmazó 1004 CBOR címke jelöl,
- d) tartalmazza az RFC 9360 szabvány szerinti x5t védett fejléc paramétert, amely SHA-256 hasító algoritmust alkalmaz a DER-kódolt végfelhasználói QSealC-tanúsítványra, valamint
- e) tömörített, és az ED1:MDOC: karakterláncot tartalmazó előtaggal van ellátva a QR-kódban való kódolás előtt.

```
{  
  
  // JSON-style, human-readable EDC logical view only.  
  
  // Actual QR payload is deterministic CBOR, not JSON.  
  
  "docType": "eu.edc", // EDC credential. The docType value is included, together with  
    //issuerSigned, in the COSE_Sign1 external payload.  
  
  "issuerSigned": {  
    // Data protected by issuerAuth; used as detached payload.  
  
    // For signature generation and verification, the detached external payload covers both  
    // docType and issuerSigned.  
  
    "nameSpaces": {  
      "eu.edc": {  
        "ver": "1.0", // QR profile/schema version  
  
        // Card serial number; issuer-defined, max. 24 characters.  
        "sub": "AB12345678901234567890CD",  

```

```

// Revocation identifier: actual CBOR bstr, 16 bytes/128 bits.
// Shown here as 32 hex characters for readability.
"rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

"givenName": "Anna", // first name printed on the EDC
"familyName": "Nagy", // surname printed on the EDC

// Actual CBOR encoding uses tag 1004 for RFC 3339 full-date.
"exp": "2030-12-31"
}
}
},

"issuerAuth": {
// Actual form: untagged COSE_Sign1, not a JSON object.
"type": "COSE_Sign1",
"tagged": false, // encoded without COSE_Sign1 CBOR tag
"payload": "detached", // COSE payload field is CBOR null

"protectedHeader": {
// alg: ES256; equivalent COSE header parameter 1 = -7.
"alg": "ES256",

// x5t: certificate thumbprint; COSE header parameter 34.
"x5t": {
"hashAlg": "SHA-256", // equivalent COSE hash value -16

```

```
// SHA-256 hash of DER-encoded end-entity QSealC.

// 32 bytes represented as 64 hex characters.

"hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

},

"unprotectedHeader": {}, // empty in this example

// ES256 COSE signature: 64 bytes = 128 hex characters.

"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"

}

}
```

9. Kriptográfiai mechanizmusok használata

A kriptográfiai mechanizmusok e melléklettel összefüggésben történő használatának összhangban kell lennie az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az Európai Unió Kiberbiztonsági Ügynökség (ENISA) által közzétett elfogadott kriptográfiai mechanizmusokkal.

II. MELLÉKLET

A FOGYATÉKOSSÁGGAL ÉLŐ SZEMÉLYEK EURÓPAI PARKOLÁSI KÁRTYÁJA FIZIKAI VÁLTOZATÁN TALÁLHATÓ QR-KÓDRA VONATKOZÓ ELŐÍRÁSOK

1. **A fogyatékossgal élő személyek európai parkolási kártyája fizikai változatán található QR-kód formátuma**
 - (a) **2. modell szerinti QR-kód formátum**, az ISO/IEC 18004:2024 vagy azzal egyenértékű nemzetközi QR-kód-specifikációknak megfelelően.
 - (b) **M hibajavítási szint** (15 %-os redundancia), amely biztosítja a nyomtatott QR-kód karcolásokkal vagy részleges károsodásával szembeni ellenálló képességet.
 - (c) **Kódolási mód**: A QR-kódban foglalt hasznos információ az issuerSigned tömör binárisobjektum-reprezentációs (CBOR) struktúra és a megfelelő issuerAuth COSE_Sign1 aláírási objektum kombinációjából áll, a CBOR-objektum aláírásban és titkosításban (a továbbiakban: COSE, RFC 9052 szabvány 3.1., 4.2. és 4.4. szakasz) meghatározottak szerint, amely az issuerSigned tételek esetében az mDOC adatmodellt követi, de hozzá van igazítva a statikus fizikai kártya használatához. Az issuerAuth egy COSE_Sign1 objektum, és egy x5t fejléc paramétert (a COSE X.509 tanúsítvány az RFC 9360 szabványban (2. szakasz) meghatározott hasítófüggvény fejléc paramétere) tartalmazó alg = ES256 algoritmus; az interoperabilitás érdekében az x5t fejléc paraméterben alkalmazott hash algoritmus az SHA-256.
 - (d) A QR-kód kódolása előtt a kombinált CBOR/COSE objektumot **zlib formátum alkalmazásával tömöríteni kell (RFC 1950 szabvány, 2.2. szakasz) a Deflate algoritmussal** (RFC 1951 szabvány, 3.2. és 4. szakasz). Az így kapott tömörített bájtömböt a **QR-kódban bájt módban** kell kódolni, biztosítva a bináris CBOR/COSE hasznos adatok és a szkanner interoperabilitásának teljes körű támogatását.

A kibocsátóknak a QR-kódban foglalt hasznos adatokban szereplő valamennyi szövegmező esetében UTF-8 Unicode karaktereket kell kódolniuk a CBOR szövegsorokon belül. Az aláírt hasznos adatokra nem alkalmazható átírás. Az interoperabilitás érdekében a kibocsátóknak az aláírás előtt minden szöveges mezőben az Unicode C normalizációs formát (NFC) kell alkalmazniuk.
 - (e) **Előtag**: A fogyatékossgal élő személyek európai parkolási kártyáján található QR-kód karakterlánc az „EP1:MDOC:” kóddal kezdődik. Ez a kártyatípust és a kódolási profilt azonosítja. Az előtagoknak különbséget kell lenniük a kis- és nagybetűk között, és meg kell jelenniük. Az ismeretlen vagy nem támogatott előtagok elutasítást eredményeznek. Az előtagot és a tömörített hasznos adatokat egyetlen bájt mód adatszégmenschént kell kódolni a QR-kódban.
 - (f) A **modul legkisebb mérete $\geq 0,35$ mm** a nyomtatott kártyák olvashatóságának biztosítása érdekében.
 - (g) **Maximális Verzió: 20**; mindkét oldalon legfeljebb 97 x 97 mm-s modullal.
2. **A fogyatékossgal élő személyek európai parkolási kártyájának aláírás-generálási előírásai**

A fogyatékossgal élő személyek európai parkolási kártyáján található QR-kódok bélyegzésére használt minősített elektronikus bélyegző (QSeal) biztosítja, hogy a kódolt adatok az engedélyezett kibocsátó hatóságtól származnak, és azokat nem módosították.

- (a) **Aláírási algoritmus:** Az aláírási algoritmus az ES256 (ECDSA, a P-256 görbét alkalmazó SHA-256 hash algoritmussal együtt), az RFC 9053 szabvány (2.1. szakasz) meghatározása szerint; a COSE-ben az algoritmust az RFC 9052 (3.1. szakasz) szabványban meghatározott algoritmikus fejléc-paraméterével azonosítják.
- (b) **Aláírási kulcs:** A QR-kódban foglalt hasznos adatokat az elektronikus bélyegző minősített tanúsítványának (QSealC) megfelelő titkos kulcs használatával kell aláírni.
- (c) **COSE-struktúra:** Az aláírás-konténernek a COSE_Sign1 objektumnak kell lennie. A védett fejlécnek az (ES256) algoritmust és az x5t fejléc paramétert (a COSE X.509 tanúsítvány RFC 9360 szabványban (2. szakasz) meghatározott hasítófüggvény fejléc paramétert) kell tartalmaznia; az interoperabilitás érdekében az x5t fejléc paraméterben alkalmazott hash algoritmus az SHA-256. A hitelesítés során az x5t értéket kell használni a megfelelő tanúsítvány keresésére a hitelesítőnek a megbízható szolgáltatók listájában szereplő információkból álló helyi bizalmi tárolójában, majd az eIDAS bizalmi keretrendszerrel összhangban hitelesíteni kell a tanúsítványláncot és a tanúsítvány státuszát.
- (d) **Aláírás Standard:** A QR-kódban foglalt hasznos adatokat COSE_Sign1 objektumként kell aláírni az RFC 9052 szabványnak (4. szakasz), a CBOR-objektumaláírásnak és titkosításnak megfelelően. A COSE_Sign1 objektumot az issuerAuth tárolja, és azt a COSE_Sign1-t jelölő CBOR-címke nélkül kell kódolni. A COSE_Sign1 objektum hasznos adatmezőjét le kell választani, és üres CBOR értéként kell kódolni. Az aláírás létrehozása és ellenőrzése esetében a külső hasznos adattartalom a determinisztikus CBOR-kódolt CBOR-szerkezet, amely tartalmazza a felső szintű CBOR kulcs-érték párokban (map) szereplő docType értéket és issuerSigned értéket.
- (e) **Hash Algoritmus:** Az aláírások generálásához és az integritás ellenőrzéséhez az ES256 algoritmus részét képező SHA-256 hash algoritmust használják.
- (f) **Kódolás:** A hasznos adatokat a tömör binárisobjektum-reprezentáció (CBOR) (RFC 8949 szabvány, 4.2. szakasz) alkalmazásával kell kódolni, a COSE- és mDOC-előírásoknak megfelelően, biztosítva az aláírt adatok kódolását és reprodukálhatóságát.

3. Nyomtatási előírások

- (a) **Világos mező:** A QR-kód minden oldalán **4 modulból** álló világos mezőt kell hagyni, amelyen nem szerepel nyomtatás, minta vagy háttérszín.
- (b) **Kontraszt:** A QR-kódot fehér háttérre kell nyomtatni, legalább **4:1** kontrasztarány mellett, hogy változó világítási körülmények között is könnyen olvasható legyen.
- (c) A QR-kódot az (EU) 2024/2841 irányelv II. mellékletében meghatározott szín használatával kell nyomtatni, amely biztosítja a maximális kontrasztot.
- (d) **Elhelyezés és méret:** A QR-kódnak a világos mezővel együtt **37 mm × 37 mm** méretűnek kell lennie, és a kártya elülső oldalán, a közepétől kissé jobbra, az alsó

széléhez közel kell azt elhelyezni. A QR-kód legfeljebb a 20. verzió (97 × 97 modul) megfelelő lehet, 0,35 mm-es vagy annál nagyobb modulmérettel.

A QR-kódot a világos mezővel együtt a kártya alsó szélétől legalább 5 mm-re kell elhelyezni.

4. **A fogyatékossgal élő személyek európai parkolási kártyáján található QR-kódban szereplő adatok**

A QR-kódnak tartalmaznia kell egy minimális, offline ellenőrizhető adatkészletet az (EU) 2016/679 rendelet 5. cikke (1) bekezdésének c) pontjában szereplő adattakarékosság elvének megfelelően. A hasznos adatok szerkezete a következő:

- (a) A kártyaattribútumokat az issuerSigned objektumon belül kódolják a CBOR-ban.
- (b) Ezt a struktúrát a kibocsátó hatóság issuerAuth-ként (COSE_Sign1, x5t hash algoritmust tartalmazó ES256 algoritmus, a COSE X.509 tanúsítvány hash fejléc paramétere) minősített elektronikus bélyegzővel (QSeal) csomagolja be és írja alá.
- (c) A létrejövő CBOR/COSE objektumot e melléklet 1. d) pontjának megfelelően tömöríteni kell. A QR-kódban foglalt hasznos információ az „EP1:MDOC:” előtagból és az utána következő, létrejövő tömörített bájtömbből áll, és a teljes hasznos adattartalmat bájtömbben, egyetlen QR-kód adatszégmengként kell kódolni.

Az adattartalom az (EU) 2024/2841 irányelv II. mellékletében felsorolt, a kártya előlapján található mezőkben szereplő látható adatok részhalmazából (lejáratási idő, dátum, a kártya sorozatszám), valamint a visszavonási azonosítóból, az elektronikus aláírásból és a sémainformációból áll.

Az **elektronikus aláírásnak** a következőket kell tartalmaznia:

- i. issuerAuth – A kibocsátó hatóság **QSealC titkos kulcsával** aláírt COSE_Sign1 objektum.
- ii. Védett fejléc, amely tartalmazza az alg = ES256 (aláírási algoritmus) és x5t (a COSE X.509 tanúsítvány hash fejléc paramétere) értéket.

5. **Opcionális adatok**

A QR-kód nem tartalmazhat opcionális adatokat.

6. **Visszavonási azonosító**

A fogyatékossgal élő személyek európai parkolási kártyáján szereplő visszavonási azonosítónak meg kell felelnie az I. melléklet 6. pontjának.

A fogyatékossgal élő személyek visszavont európai parkolási kártyáira vonatkozó visszavonási jegyzékekben csak a visszavonási azonosító szerepelhet. A kártya sorozatszámait nem tehetők közzé a visszavonási jegyzékekben.

7. **A fogyatékossgal élő személyek európai parkolási kártyáján található tömör binárisobjektum-reprezentációban (CBO) szereplő hasznos adatok (a QR-kódon belül)**

A QR-kódban foglalt hasznos adatokon belül csak a következő adatok tüntethetők fel, amelyek megfelelnek a fogyatékossgal élő személyek európai parkolási kártyájának az (EU) 2024/2841 irányelv II. mellékletében meghatározott látható adatmezőivel.

Mező	mDOC path	Típus/Formátum
Adatséma verzió	issuerSigned.nameSpaces."eu.epc".ver	Karakterlánc (pl. „1.0”)
Kártya típusa: A fogyatékossgal élő személyek európai parkolási kártyája	docType	Enum ("eu.epc")
A kártya sorozatszám	issuerSigned.nameSpaces."eu.epc".sub	Karakterlánc
Visszavonási azonosító	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 bájtt)
A kártya érvényessége	issuerSigned.nameSpaces."eu.epc".exp	az RFC 8943 szabványban (2.1. szakasz) meghatározott 1004 CBOR-címke, amely egy, az RFC 3339 szabványnak megfelelő, ÉÉÉ-HH-NN formátumú teljes dátumot reprezentáló UTF-8 szövegsort tartalmaz

Az elektronikus aláírást az issuerAuth (COSE_Sign1 objektum) tárolja. A tanúsítványlánc nem építhető be a QR-kód hasznos adattartalmába; ehelyett a védett COSE fejlécnek tartalmaznia kell az x5t tanúsítvány ujjlenyomat-algoritmust, amely arra szolgál, hogy a hitelesítő gyorsítótárazott bizalmi tárolójában megtalálható legyen a megfelelő QSealC-tanúsítvány.

8. **A fogyatékossgal élő személyek európai parkolási kártyáján található QR-kódban foglalt hasznos adatok példája: JavaScript Objektum Jelölés stílusú kommentált logikai reprezentáció**

A következő példa a fogyatékosággal élő személyek európai parkolási kártyája logikai nézetének ember által olvasható JavaScript Objektum Jelölés (JSON) reprezentációja. A gyakorlatban ez a struktúra nem lehet ember által olvasható, mivel:

- (a) CBOR-ban van kódolva (RFC 8949 szabvány, 3. szakasz),
- (b) jelölés nélküli COSE_Sign1 szerkezet alkalmazásával van aláírva, és a hasznos adattartalom le van választva (RFC 9052 szabvány, 4. szakasz),
- (c) lejárat dátumot tartalmaz, amelyet az RFC 8943 szabvány (2.1. szakasz) szerinti, teljes dátum értéket tartalmazó 1004 CBOR címke jelöl,
- (d) tartalmazza az RFC 9360 szabvány szerinti x5t védett fejléc paramétert, amely SHA-256 hasító algoritmust alkalmaz a DER-kódolt végfelhasználói QSealC-tanúsítványra, valamint
- (e) tömörített, és az EP1:MDOC: karakterláncot tartalmazó előtaggal van ellátva a QR-kódban való kódolás előtt.

```
{  
  // JSON-style, human-readable EPC logical view only.  
  // Actual QR payload is deterministic CBOR, not JSON.  
  "docType": "eu.epc", // EPC credential. The docType value is included, together with  
    //issuerSigned, in the COSE_Sign1 external payload.  
  
  "issuerSigned": {  
    // Data protected by issuerAuth; used as detached payload.  
  
    // For signature generation and verification, the detached external payload covers both  
    // docType and issuerSigned.  
  
    "nameSpaces": {  
      "eu.epc": {  
        "ver": "1.0", // QR profile/schema version  
  
        // Card serial number; issuer-defined, max. 24 characters.  
        "sub": "EF12345678901234567890GH",  
  
        // Revocation identifier: actual CBOR bstr, 16 bytes/128 bits.
```

```

// Shown here as 32 hex characters for readability.
"rid": "4a8d9c112233445566778899aabbccdd",

// Actual CBOR encoding uses tag 1004 for RFC 3339 full-date.
"exp": "2030-12-31"
}
}
},

"issuerAuth": {
// Actual form: untagged COSE_Sign1, not a JSON object.
"type": "COSE_Sign1",
"tagged": false, // encoded without COSE_Sign1 CBOR tag
"payload": "detached", // COSE payload field is CBOR null

"protectedHeader": {
// alg: ES256; equivalent COSE header parameter 1 = -7.
"alg": "ES256",

// x5t: certificate thumbprint; COSE header parameter 34.
"x5t": {
"hashAlg": "SHA-256", // equivalent COSE hash value -16

// SHA-256 hash of DER-encoded end-entity QSealC.
// 32 bytes represented as 64 hex characters.
"hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
}
}
}

```

```
},
```

```
"unprotectedHeader": {}, // empty in this example
```

```
// ES256 COSE signature: 64 bytes = 128 hex characters.
```

```
"signature":
```

```
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc  
def0123456789abcdef0123456789abcdef0123456789abcdef"
```

```
}
```

```
}
```

9. Kriptográfiai mechanizmusok használata

A kriptográfiai mechanizmusok e melléklettel összefüggésben történő használatának összhangban kell lennie az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az Európai Unió Kiberbiztonsági Ügynökség (ENISA) által közzétett elfogadott kriptográfiai mechanizmusokkal.

III. MELLÉKLET

ÉRTESÍTÉS A 6. CIKK (2) BEKEZDÉSÉBEN EMLÍTETT INFORMÁCIÓKRÓL

1. A tagállamok a következő információkat szolgáltatják a Bizottságnak az európai fogyatékosági kártya és a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatának kiállításáért felelős minden egyes illetékes hatóságról vagy szervről:
 - (a) az európai fogyatékosági kártya és a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatának kiállításáért felelős minden egyes illetékes hatóság vagy szerv neve;
 - (b) az európai fogyatékosági kártya és a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatának kiállításáért felelős minden egyes illetékes hatóság vagy szerv regisztrációs száma;
 - (c) az európai fogyatékosági kártya és a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatának kiállításáért felelős minden egyes illetékes hatóság vagy szerv kapcsolattartási e-mail-címe és telefonszáma;
 - (d) az európai fogyatékosági kártya vagy a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatának kiállításáért felelős illetékes hatóság vagy szerv által létrehozott elektronikus bélyegző ellenőrzésére felhasználható, az érintett hatóság vagy szerv által kiadott egy vagy több tanúsítvány, amelyben szereplő hitelesített személyazonosító adatok – az a), illetve a b) pontban meghatározottak szerint – tartalmazzák a kibocsátó nevét, illetve regisztrációs számát;
 - (e) annak a helynek a webcíme, ahol a kibocsátó közzéteszi az európai fogyatékosági kártya és a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatának érvényességi állapotát.
2. A tagállamok a következő információkat szolgáltatathatják a Bizottságnak az európai fogyatékosági kártya és a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatának kiállításáért felelős minden egyes illetékes hatóságról vagy szervről:
 - (a) azon weboldal webcíme, amely tartalmazza az európai fogyatékosági kártya vagy a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatának kiállításáért felelős illetékes hatóság vagy szerv azon szabályzatait és feltételeit, amelyek az európai fogyatékosági kártya és a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatának rendelkezésre bocsátására és használatára vonatkoznak;
 - (b) adott esetben azon weboldal webcíme, amely kiegészítő információkat tartalmaz az európai fogyatékosági kártya és a fogyatékosággal élő személyek európai parkolási kártyája fizikai változatának kiállításáért felelős illetékes hatóságra vagy szervre vonatkozóan.


```
(tstr / int) => RFU
}

Identifier = bstr

Aggregation_uri = tstr
```