

Bruselj, 10. julij 2026  
(OR. en)

11772/26  
ADD 1

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

## SPREMNI DOPIS

|                |                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pošiljatelj:   | za generalno sekretarko Evropske komisije:<br>direktorica Martine DEPREZ                                                                                                                                                                                                                                                                                             |
| Datum prejema: | 1. julij 2026                                                                                                                                                                                                                                                                                                                                                        |
| Prejemnik:     | Thérèse BLANCHET, generalna sekretarka Sveta Evropske unije                                                                                                                                                                                                                                                                                                          |
| Št. dok. Kom.: | C(2026) 4534 annex                                                                                                                                                                                                                                                                                                                                                   |
| Zadeva:        | PRILOGE<br>k<br>DELEGIRANI UREDBI KOMISIJE (EU) .../...<br>o dopolnitvi Direktive (EU) 2024/2841 glede določitve kode QR na fizični različici evropske kartice ugodnosti za invalide ter določitve kode QR in skupnih tehničnih specifikacij, ki zagotavljajo varnost fizične različice evropske parkirne karte za invalide, ter zadev v zvezi z interoperabilnostjo |



EVROPSKA  
KOMISIJA

Bruselj, 1.7.2026  
C(2026) 4534 final

ANNEXES 1 to 4

## **PRILOGE**

**k**

**DELEGIRANI UREDBI KOMISIJE (EU) .../...**

**o dopolnitvi Direktive (EU) 2024/2841 glede določitve kode QR na fizični različici evropske kartice ugodnosti za invalide ter določitve kode QR in skupnih tehničnih specifikacij, ki zagotavljajo varnost fizične različice evropske parkirne karte za invalide, ter zadev v zvezi z interoperabilnostjo**

## PRILOGA I

### SPECIFIKACIJE ZA KODO QR ZA FIZIČNO RAZLIČICO EVROPSKE KARTICE UGODNOSTI ZA INVALIDE

1. **Oblika kode QR za fizično različico evropske kartice ugodnosti za invalide (EDC)**
  - (a) **Oblika kode QR model 2** v skladu z mednarodnimi specifikacijami za kode QR ISO/IEC 18004:2024 ali enakovrednimi standardi.
  - (b) **Stopnja odpravljanja napak M** (15-odstotna redundanca), ki zagotavlja odpornost proti praskam ali delni poškodbi natisnjene kode QR.
  - (c) **Način kodiranja:** Koristna vsebina QR je sestavljena iz kombinirane issuerSigned strukture strnjene predstavitve binarnega objekta (CBOR) in ustreznega objekta podpisa issuerAuth COSE\_Sign1, kot je opredeljen v podpisovanju in šifriranju objekta s CBOR (COSE, RFC 9052, oddelki 3.1, 4.2 in 4.4), v skladu z vzorcem podatkovnega modela mDOC za elemente issuerSigned, vendar prilagojena za uporabo na statičnih fizičnih karticah. IssuerAuth je objekt COSE\_Sign1 z alg = ES256 in zaščiteno glavo, ki vsebuje x5t (parameter zgoščevalne glave certifikata COSE X.509, opredeljen v RFC 9360 (oddelek 2); za interoperabilnost se v x5t uporablja zgoščevalni algoritem SHA-256).
  - (d) Pred kodiranjem kode QR se združeni objekt CBOR/COSE **kompresira z uporabo formata zlib** (RFC 1950, oddelek 2.2) z algoritmom **deflate** (RFC 1951, oddelka 3.2 in 4). Dobljena kompresirana vrsta bajtov se kodira v **bajtni način kode QR**, s čimer se zagotovi popolna podpora za binarne koristne vsebine CBOR/COSE in interoperabilnost optičnega bralnika.

Izdajatelji za vsa besedilna polja, vključena v koristno vsebino QR, v besedilnih nizih CBOR kodirajo znake kot Unicode UTF-8. Prečrkovanje se ne uporablja za podpisane podatke koristne vsebine. Za namene interoperabilnosti izdajatelji pred podpisom uporabijo obrazec za standardizacijo Unicode C (NFC) za vsa besedilna polja.
  - (e) **Predpona:** Niz QR evropske kartice ugodnosti za invalide se začne z „ED1:MDOC:“. To označuje vrsto kartice in profil kodiranja. Predpone razlikujejo med malimi in velikimi črkami in morajo biti prisotne. Neznane ali nepodprte predpone povzročijo zavrnitev. Predpona in kompresirana koristna vsebina sta v kodi QR kodirana kot en podatkovni segment v bajtnem načinu.
  - (f) **Najmanjša velikost modula  $\geq 0,25$  mm**, da se zagotovi berljivost na tiskanih karticah.
  - (g) **Največja različica 20**; z do  $97 \times 97$  moduli na vsaki strani.

### 2. **Specifikacije za generiranje podpisa evropske kartice ugodnosti za invalide**

Kvalificirani elektronski žig (QSeal), ki se uporablja za žigosanje kod QR evropske kartice ugodnosti za invalide, zagotavlja, da kodirani podatki izvirajo od pooblaščenega organa izdajatelja in niso bili spremenjeni.

- (a) **Algoritem podpisa:** Algoritem podpisa je ES256 (algoritem digitalnega podpisa na podlagi eliptične krivulje (ECDSA) s SHA-256 z uporabo krivulje P-256), kot je

opredeljeno v RFC 9053 (oddelek 2.1); v COSE je algoritem identificiran s parametrom glave alg v RFC 9052 (oddelek 3.1).

- (b) **Ključ za podpisovanje:** Koristna vsebina QR se podpiše z zasebnim ključem, ki ustreza kvalificiranemu potrdilu za elektronski žig (QSealC).
- (c) **Struktura COSE:** Vsebnik podpisov je objekt COSE\_Sign1. Zaščiten glava vsebuje alg (ES256) in x5t (parameter zgoščevalne glave certifikata COSE X.509, opredeljen v RFC 9360 (oddelek 2); za interoperabilnost se v x5t uporablja zgoščevalni algoritem SHA-256). Preverjanje temelji na uporabi vrednosti x5t za lociranje ustreznega certifikata v lokalno predpomnjeni shrambi zaupanja vrednih potrdil preveritelja, vzpostavljeni na podlagi informacij z zanesljivega seznama, nato pa se potrdita veriga certifikatov in status certifikata v skladu z okvirom zaupanja eIDAS.
- (d) **Standard za podpis:** Koristna vsebina kode QR se podpiše kot objekt COSE\_Sign1 v skladu z RFC 9052 (oddelek 4), podpisovanje in šifriranje objekta s CBOR. Objekt COSE\_Sign1 je v issuerAuth in je kodiran brez oznake CBOR za COSE\_Sign1. Polje za koristno vsebino objekta COSE\_Sign1 je ločeno in kodirano kot CBOR null. Za ustvarjanje in preverjanje podpisa je zunanja koristna vsebina deterministično kodirana struktura CBOR, ki vsebuje vrednost docType in vrednost issuerSigned s sheme CBOR najvišje ravni.
- (e) **Zgoščevalni algoritem:** Za ustvarjanje podpisa in preverjanje celovitosti se uporablja SHA-256 kot del ES256.
- (f) **Kodiranje:** Koristna vsebina se kodira z uporabo CBOR (RFC 8949, oddelek 4.2), kot se zahteva v specifikacijah COSE in mDOC, da se zagotovita kodiranje in ponovljivost podpisanih podatkov.

### 3. Specifikacije za tisk

- (a) **Tiha cona:** Kodo QR na vseh straneh obdaja prazen rob **štirih modulov** brez kakršnega koli tiska, vzorca ali ozadja.
- (b) **Kontrast:** Koda QR je natisnjena na belem ozadju s kontrastnim razmerjem najmanj **4:1**, da se zagotovi visoka berljivost v različnih pogojih osvetlitve.
- (c) Koda QR se natisne v barvi, opredeljeni v Prilogi I k Direktivi (EU) 2024/2841, ki zagotavlja največji kontrast.
- (d) **Postavitev in velikost:** Koda QR, vključno s tiho cono, je velikosti 26,25 mm × 26,25 mm in se nahaja na hrbtni strani kartice v spodnjem desnem kotu. Koda QR je največje različice 20 (97 × 97 modulov) z velikostjo modula 0,25 mm ali več.

Koda QR, vključno z njeno tiho cono, je nameščena najmanj 5 mm od desnega roba in najmanj 5 mm od spodnjega roba kartice.

### 4. Podatki v kodi QR evropske kartice ugodnosti za invalide

Koda QR vsebuje minimalen nabor podatkov, ki ga je mogoče preveriti brez povezave, v skladu z načelom najmanjšega obsega podatkov iz člena 5(1), točka (c), Uredbe (EU) 2016/679. Struktura koristne vsebine je naslednja:

- (a) Atributi kartice so kodirani v CBOR v objektu issuerSigned.

- (b) Strukturo zavije in podpiše QSeal organa izdajatelja kot issuerAuth (COSE\_Sign1, ES256, vključno z x5t, ki je parameter zgoščevalne glave certifikata COSE X.509).
- (c) Nastali objekt CBOR/COSE se kompresira v skladu s točko 1(d) te priloge. Koristno vsebino kode QR sestavljata predpona „ED1:MDOC:“, ki ji sledi dobljena kompresirana vrsta bajtov, celoten koristen tovor pa se kodira z uporabo bajtnega načina kot en sam podatkovni segment kode QR.

Vsebina podatkov je sestavljena iz podniza vidnih podatkov iz polj na sprednji strani kartice iz Priloge I k Direktivi (EU) 2024/2841 (ime, priimek, serijska številka kartice, datum izteka veljavnosti), skupaj z identifikatorjem preklica, elektronskim podpisom in informacijami o shemi.

#### **Elektronski podpis** vsebuje:

- (i) issuerAuth – objekt COSE\_Sign1, podpisan z **zasebnim ključem QSealC** organa izdajatelja;
- (ii) zaščiteno glavo, ki vključuje alg = ES256 (algoritem podpisa) in x5t (parameter zgoščevalne glave certifikata COSE X.509).

### **5. Neobvezni podatki**

V kodo QR se ne vključijo nobeni neobvezni podatki.

### **6. Identifikator preklica (RID)**

Poleg vidne serijske številke kartice koda QR vključuje namenski identifikator preklica (RID).

RID se uporablja za ugotavljanje statusa preklica in upravljanje seznama preklicev. RID se ne natisne na kartico in se ne prikaže preveriteljem kartice.

#### *6.1. Zahteve za RID*

RID:

- (a) je vključen v podpisano koristno vsebino QR;
- (b) je edinstven vsaj znotraj domene izdaje organa izdajatelja;
- (c) ni natisnjen na kartici in ni namenjen, da bi bil človeku berljiv;
- (d) ne razkriva osebnih podatkov in nima neposrednega pomena;
- (e) ni ga mogoče neposredno razbrati iz vidne serijske številke kartice in
- (f) je kriptografsko vezan na koristno vsebino QR s kvalificiranim elektronskim žigom.

#### *6.2. Oblika in velikost RID*

RID se kodira kot bajtni niz CBOR (bstr). RID je dolg 16 bajtov (128 bitov).

RID ustvari organ izdajatelj z uporabo metode, ki je pod njegovim nadzorom ter zagotavlja zadostno entropijo in odpornost proti ugibanju ali štetju.

#### *6.3. Sezname preklicev*

Sezname preklicev, objavljeni za namene preverjanja, navajajo le RID preklicanih kartic. Serijske številke kartic se ne objavijo na seznamih preklicev.

## 7. Koristna vsebina CBOR (znotraj kode QR) evropske kartice ugodnosti za invalide

V koristno vsebino QR se vključijo samo naslednji podatki, skladni z vidnimi podatkovnimi polji evropske kartice ugodnosti za invalide iz Priloge I k Direktivi (EU) 2024/2841.

Vsebina najvišje ravni:

- (a) docType = "eu.edc"
- (b) issuerSigned.nameSpaces."eu.edc" z atributi, prikazanimi v tabeli spodaj
- (c) issuerAuth = COSE\_Sign1 (QSeal)

| Polje                            | pot mDOC                                    | Vrsta/oblika                                                                                                                                                 |
|----------------------------------|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Različica sheme podatkov         | issuerSigned.nameSpaces."eu.edc".ver        | niz (npr. "1.0")                                                                                                                                             |
| Vrsta kartice: EDC               | docType                                     | Enum ("eu.edc")                                                                                                                                              |
| Serijska številka kartice        | issuerSigned.nameSpaces."eu.edc".sub        | niz                                                                                                                                                          |
| Identifikator preklica           | issuerSigned.nameSpaces."eu.edc".rid        | CBOR bstr (16 bajtov)                                                                                                                                        |
| Ime imetnika kartice             | issuerSigned.nameSpaces."eu.edc".givenName  | besedilni niz Unicode (UTF-8)                                                                                                                                |
| Priimek imetnika kartice         | issuerSigned.nameSpaces."eu.edc".familyName | besedilni niz Unicode (UTF-8)                                                                                                                                |
| Datum izteka veljavnosti kartice | issuerSigned.nameSpaces."eu.edc".exp        | Oznaka CBOR 1004, kot je opredeljena v RFC 8943 (oddelek 2.1) in ki vsebuje besedilni niz UTF-8, ki predstavlja polni datum RFC 3339<br>v obliki LLLL-MM-DD. |

Elektronski podpis je v issuerAuth (objekt COSE\_Sign1). Veriga certifikatov ni vgrajena v koristno vsebino kode QR; namesto tega zaščitena glava COSE vključuje x5t, torej razpoznavni odtis certifikata, ki se uporablja za lociranje ustreznega QSealC v predpomnjeni shrambi zaupanja vrednih potrdil preveritelja.

## 8. Primer koristne vsebine kode QR evropske kartice ugodnosti za invalide: logični prikaz v obliki JavaScript Object Notation s komentarji

Naslednji primer ponazarja človeku berljiv prikaz v obliki JavaScript Object Notation (JSON) logičnega pregleda evropske kartice ugodnosti za invalide. V praksi ta struktura ni človeku berljiva, saj:

- (a) je kodirana v CBOR (RFC 8949, oddelek 3);
- (b) je podpisana z uporabo neoznačene strukture COSE\_Sign1 z ločeno koristno vsebino (RFC 9052, oddelek 4);
- (c) vključuje datum izteka veljavnosti kot oznako CBOR 1004 z vrednostjo za polni datum v skladu z RFC 8943 (oddelek 2.1);
- (d) vključuje parameter zaščitene glave x5t v skladu z RFC 9360, pri čemer uporablja SHA-256 prek z DER kodiranega QSealC končnega subjekta, in
- (e) je kompresirana in se ji doda predpona z nizom ED1:MDOC:, preden se kodira v kodo QR.

```
{
```

```
  // v obliki JSON, samo logični prikaz evropske kartice ugodnosti za invalide v človeku berljivi obliki.
```

```
  // dejanska koristna vsebina QR je deterministični CBOR in ne JSON.
```

```
  "docType": "eu.edc", // potrdilo evropske kartice ugodnosti za invalide. Vključena je vrednost docType, skupaj z
```

```
    //issuerSigned v zunanji koristni vsebini COSE_Sign1.
```

```
  "issuerSigned": {
```

```
    // Podatki, zaščiteni z issuerAuth; uporabljajo se kot ločena koristna vsebina.
```

```
    // Za ustvarjanje in preverjanje podpisa ločena zunanja koristna vsebina zajema tako
```

```
    // docType kot issuerSigned.
```

```
    "nameSpaces": {
```

```
      "eu.edc": {
```

```
        "ver": "1.0", // različica profila/sheme QR
```

```
        // Serijska številka kartice; določi izdajatelj, največ 24 znakov.
```

```
        "sub": "AB12345678901234567890CD",
```

```

// Identifikator preklica: dejanski CBOR bstr, 16 bajtov/128 bitov.

// Prikazano tukaj kot 32 hex znakov za namene berljivosti.

"rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

"givenName": "Janez", // ime, natisnjeno na evropski kartici ugodnosti za invalide
"familyName": "Vzorec", // priimek, natisnjen na evropski kartici ugodnosti za invalide


// Dejansko kodiranje CBOR uporablja oznako 1004 za polni datum RFC 3339.

"exp": "2030-12-31"

}

},

"issuerAuth": {
// Dejanska oblika: neoznačen COSE_Sign1 in ne objekt JSON.

"type": "COSE_Sign1",
"tagged": false, // kodirano brez CBOR oznake COSE_Sign1
"payload": "detached", // koristna vsebina COSE je CBOR null

"protectedHeader": {
// alg: ES256; ekvivalentni parameter glave COSE 1 = -7.

"alg": "ES256",

// x5t: razpoznavni odtis potrdila; parameter glave COSE 34

"x5t": {
"hashAlg": "SHA-256", //ekvivalent zgoščene vrednosti COSE -16

```

```

// zgoščena vrednost SHA-256 z DER kodiranega QSealC končnega subjekta.

// 32 bajtov, predstavljenih kot 64 hex znakov.

"hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef"

}

},

"unprotectedHeader": {}, // prazno v tem primeru

// podpis ES256 COSE: 64 bajtov = 128 hex znakov.

"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

```

## 9. Uporaba kriptografskih mehanizmov

Uporaba kriptografskih mehanizmov v okviru te priloge je skladna z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetiko varnost in objavila Agencija Evropske unije za kibernetiko varnost (ENISA).

## PRILOGA II

### **SPECIFIKACIJE ZA KODO QR ZA FIZIČNO RAZLIČICO EVROPSKE PARKIRNE KARTE ZA INVALIDE**

1. **Oblika kode QR na fizični različici evropske parkirne karte za invalide (EPC)**
  - (a) **Oblika kode QR model 2** v skladu z mednarodnimi specifikacijami za kode QR ISO/IEC 18004:2024 ali enakovrednimi standardi.
  - (b) **Stopnja odpravljanja napak M** (15-odstotna redundanca), ki zagotavlja odpornost proti praskam ali delni poškodbi natisnjene kode QR.
  - (c) **Način kodiranja:** Koristna vsebina QR je sestavljena iz kombinirane issuerSigned strukture strnjene predstavitve binarnega objekta (CBOR) in ustreznega objekta podpisa issuerAuth COSE\_Sign1, kot je opredeljen v podpisovanju in šifriranju objekta s CBOR (COSE, RFC 9052, oddelki 3.1, 4.2 in 4.4), v skladu z vzorcem podatkovnega modela mDOC za elemente issuerSigned, vendar prilagojena za uporabo na statičnih fizičnih kartah. IssuerAuth je objekt COSE\_Sign1 z alg = ES256 in zaščiteno glavo, ki vsebuje x5t (parameter zgoščevalne glave certifikata COSE X.509, opredeljen v RFC 9360 (oddelek 2); za interoperabilnost se v x5t uporablja zgoščevalni algoritem SHA-256).
  - (d) Pred kodiranjem kode QR se združeni objekt CBOR/COSE **kompresira z uporabo formata zlib (RFC 1950, oddelek 2.2)** z algoritmom **deflate** (RFC 1951, oddelek 3.2 in 4). Dobljena kompresirana vrsta bajtov se kodira v **bajtni način kode QR**, s čimer se zagotovi popolna podpora za binarne koristne vsebine CBOR/COSE in interoperabilnost optičnega bralnika.

Izdajatelji za vsa besedilna polja, vključena v koristno vsebino QR, v besedilnih nizih CBOR kodirajo znake kot Unicode UTF-8. Prečrkovanje se ne uporablja za podpisane podatke koristne vsebine. Za namene interoperabilnosti izdajatelji pred podpisom uporabijo obrazec za standardizacijo Unicode C (NFC) za vsa besedilna polja.
  - (e) **Predpona:** Niz QR evropske parkirne karte za invalide se začne z „EP1:MDOC:“. To označuje vrsto karte in profil kodiranja. Predpone razlikujejo med malimi in velikimi črkami in morajo biti prisotne. Neznane ali nepodprte predpone povzročijo zavrnitev. Predpona in kompresirana koristna vsebina sta v kodi QR kodirana kot en podatkovni segment v bajtnem načinu.
  - (f) **Najmanjša velikost modula  $\geq 0,35$  mm**, da se zagotovi berljivost na tiskanih kartah.
  - (g) **Največja različica 20**; z do  $97 \times 97$  moduli na vsaki strani.

### **2. Specifikacije za generiranje podpisa evropske parkirne karte za invalide**

Kvalificirani elektronski žig (QSeal), ki se uporablja za žigosanje kod QR evropske parkirne karte za invalide, zagotavlja, da kodirani podatki izvirajo od pooblaščenega organa izdajatelja in niso bili spremenjeni.

- (a) **Algoritem podpisa:** Algoritem podpisa je ES256 (ECDSA s SHA-256 z uporabo krivulje P-256), kot je opredeljeno v RFC 9053 (oddelek 2.1); v COSE je algoritem identificiran s parametrom glave alg v RFC 9052 (oddelek 3.1).

- (b) **Ključ za podpisovanje:** Koristna vsebina QR se podpiše z zasebnim ključem, ki ustreza kvalificiranemu potrdilu za elektronski žig (QSealC).
- (c) **Struktura COSE:** Vsebnik podpisov je objekt COSE\_Sign1. Zaščitena glava vsebuje alg (ES256) in x5t (parameter zgoščevalne glave certifikata COSE X.509, opredeljen v RFC 9360 (oddelek 2); za interoperabilnost se v x5t uporablja zgoščevalni algoritem SHA-256). Preverjanje temelji na uporabi vrednosti x5t za lociranje ustreznega certifikata v lokalno predpomnjeni shrambi zaupanja vrednih potrdil preveritelja, vzpostavljeni na podlagi informacij z zanesljivega seznama, nato pa se potrdita veriga certifikatov in status certifikata v skladu z okvirom zaupanja eIDAS.
- (d) **Standard za podpis:** Koristna vsebina kode QR se podpiše kot objekt COSE\_Sign1 v skladu z RFC 9052 (oddelek 4), podpisovanje in šifriranje objekta s CBOR. Objekt COSE\_Sign1 je v issuerAuth in je kodiran brez oznake CBOR za COSE\_Sign1. Polje za koristno vsebino objekta COSE\_Sign1 je ločeno in kodirano kot CBOR null. Za ustvarjanje in preverjanje podpisa je zunanja koristna vsebina deterministično CBOR kodirana struktura CBOR, ki vsebuje vrednost docType in vrednost issuerSigned s sheme CBOR najvišje ravni.
- (e) **Zgoščevalni algoritem:** Za ustvarjanje podpisa in preverjanje celovitosti se uporablja SHA-256 kot del ES256.
- (f) **Kodiranje:** Koristna vsebina se kodira z uporabo CBOR (RFC 8949, oddelek 4.2), kot se zahteva v specifikacijah COSE in mDOC, da se zagotovita kodiranje in ponovljivost podpisanih podatkov.

### 3. Specifikacije za tisk

- (a) **Tiha cona:** Kodo QR na vseh straneh obdaja prazen rob **štirih modulov** brez kakršnega koli tiska, vzorca ali ozadja.
- (b) **Kontrast:** Koda QR je natisnjena na belem ozadju s kontrastnim razmerjem najmanj **4:1**, da se zagotovi visoka berljivost v različnih pogojih osvetlitve.
- (c) Koda QR se natisne v barvi, opredeljeni v Prilogi II k Direktivi (EU) 2024/2841, ki zagotavlja največji kontrast.
- (d) **Postavitev in velikost:** Koda QR, vključno s tiho cono, je velikosti 37 mm × 37 mm in se nahaja na sprednji strani karte rahlo na desni proti spodnjemu robu. Koda QR je največje različice 20 (97 × 97 modulov) z velikostjo modula 0,35 mm ali več.  
  
Koda QR, vključno z njeno tiho cono, je nameščena najmanj 5 mm od spodnjega roba karte.

### 4. Podatki v QR kodi evropske parkirne karte za invalide

Koda QR vsebuje minimalen nabor podatkov, ki ga je mogoče preveriti brez povezave, v skladu z načelom najmanjšega obsega podatkov iz člena 5(1), točka (c), Uredbe (EU) 2016/679. Struktura koristne vsebine je naslednja:

- (a) Atributi karte so kodirani v CBOR v objektu issuerSigned.
- (b) To strukturo zavije in podpiše QSeal organa izdajatelja kot issuerAuth (COSE\_Sign1, ES256, vključno z x5t, ki je parameter zgoščevalne glave certifikata COSE X.509).

- (c) Nastali objekt CBOR/COSE se kompresira v skladu s točko 1(d) te priloge. Koristno vsebino kode QR sestavljata predpona „EPI:MDOC:“, ki ji sledi dobljena kompresirana vrsta bajtov, celoten koristen tovor pa se kodira z uporabo bajtnega načina kot en sam podatkovni segment kode QR.

Vsebina podatkov je sestavljena iz podniza vidnih podatkov iz polj na sprednji strani karte iz Priloge II k Direktivi (EU) 2024/2841 (datum izteka veljavnosti, serijska številka karte), skupaj z identifikatorjem preklica, elektronskim podpisom in informacijami o shemi.

#### **Elektronski podpis vsebuje:**

- (i) issuerAuth – objekt COSE\_Sign1, podpisan z **zasebnim ključem QSealC** organa izdajatelja;
- (ii) zaščiteno glavo, ki vključuje alg = ES256 (algoritem podpisa) in x5t (parameter zgoščevalne glave certifikata COSE X.509).

### **5. Neobvezni podatki**

V kodo QR se ne vključijo nobeni neobvezni podatki.

### **6. Identifikator preklica (RID)**

Identifikator preklica evropske parkirne karte za invalide je skladen s točko 6 Priloge I.

Seznami preklicev za preklicane evropske parkirne karte za invalide energetskih izkaznic navajajo le RID. Serijske številke kart se ne objavijo na seznamih preklicev.

### **7. Koristna vsebina CBOR (znotraj kode QR) evropske parkirne karte za invalide**

V koristno vsebino QR se vključijo samo naslednji podatki, skladni z vidnimi podatkovnimi polji evropske parkirne karte za invalide iz Priloge II k Direktivi (EU) 2024/2841.

| <b>Polje</b>                   | <b>pot mDOC</b>                      | <b>Vrsta/oblika</b>                                                         |
|--------------------------------|--------------------------------------|-----------------------------------------------------------------------------|
| Različica sheme podatkov       | issuerSigned.nameSpaces."eu.epc".ver | niz (npr. "1.0")                                                            |
| Vrsta karte:<br>EPC            | docType                              | Enum<br>("eu.epc")                                                          |
| Serijska številka karte        | issuerSigned.nameSpaces."eu.epc".sub | niz                                                                         |
| Identifikator preklica         | issuerSigned.nameSpaces."eu.epc".rid | CBOR bstr (16 bajtov)                                                       |
| Datum izteka veljavnosti karte | issuerSigned.nameSpaces."eu.epc".exp | Oznaka CBOR 1004, kot je opredeljena v RFC 8943 (oddelek 2.1) in ki vsebuje |

|  |  |                                                                                                      |
|--|--|------------------------------------------------------------------------------------------------------|
|  |  | besedilni niz<br>UTF-8, ki<br>predstavlja<br>polni datum<br>RFC 3339<br>v obliki LLLL-<br>MM-<br>DD. |
|--|--|------------------------------------------------------------------------------------------------------|

Elektronski podpis je v issuerAuth (objekt COSE\_Sign1). Veriga certifikatov ni vgrajena v koristno vsebino kode QR; namesto tega zaščitena glava COSE vključuje x5t, torej razpoznavni odtis certifikata, ki se uporablja za lociranje ustreznega QSealC v predpomnjeni shrambi zaupanja vrednih potrdil preveritelja.

#### 8. Primer koristne vsebine kode QR evropske parkirne karte za invalide: logični prikaz v obliki JavaScript Object Notation s komentarji

Naslednji primer ponazarja človeku berljiv prikaz v obliki JavaScript Object Notation (JSON) logičnega pregleda evropske parkirne karte za invalide. V praksi ta struktura ni človeku berljiva, saj je:

- (a) kodirana v CBOR (RFC 8949, oddelek 3),
- (b) je podpisana z uporabo neoznačene strukture COSE\_Sign1 z ločeno koristno vsebino (RFC 9052, oddelek 4);
- (c) vključuje datum izteka veljavnosti kot oznako CBOR 1004 z vrednostjo za polni datum v skladu z RFC 8943 (oddelek 2.1);
- (d) vključuje parameter zaščitene glave x5t v skladu z RFC 9360, pri čemer uporablja SHA-256 prek z DER kodiranega QSealC končnega subjekta, in
- (e) je kompresirana in se ji doda predpona z nizom EP1:MDOC:, preden se kodira v kodo QR.

```
{
```

```
// v obliki JSON, samo logični prikaz evropske parkirne karte za invalide v človeku berljivi obliki.
```

```
// dejanska koristna vsebina QR je deterministični CBOR in ne JSON.
```

```
"docType": "eu.epc", // potrdilo evropske parkirne karte za invalide. Vključena je vrednost docType, skupaj z
```

```
//issuerSigned v zunanji koristni vsebini COSE_Sign1.
```

```
"issuerSigned": {
```

```

// Podatki, zaščiteni z issuerAuth; uporabljajo se kot ločena koristna vsebina.

// Za ustvarjanje in preverjanje podpisa ločena zunanja koristna vsebina zajema tako
// docType kot issuerSigned.

"nameSpaces": {
  "eu.epc": {
    "ver": "1.0", // različica profila/scheme QR

    // Serijska številka karte; določi izdajatelj, največ 24 znakov.
    "sub": "EF12345678901234567890GH",

    // Identifikator preklica: dejanski CBOR bstr, 16 bajtov/128 bitov.
    // Prikazano tukaj kot 32 hex znakov za namene berljivosti.
    "rid": "4a8d9c112233445566778899aabbccdd",

    // Dejansko kodiranje CBOR uporablja oznako 1004 za polni datum RFC 3339.
    "exp": "2030-12-31"
  }
},

"issuerAuth": {
  // Dejanska oblika: neoznačen COSE_Sign1 in ne objekt JSON.
  "type": "COSE_Sign1",
  "tagged": false, // kodirano brez CBOR oznake COSE_Sign1
  "payload": "detached", // koristna vsebina COSE je CBOR null

  "protectedHeader": {

```

```

// alg: ES256; ekvivalentni parameter glave COSE 1 = -7.
"alg": "ES256",

// x5t: razpoznavni odtis potrdila; parameter glave COSE 34
"x5t": {
  "hashAlg": "SHA-256", //ekvivalent zgoščene vrednosti COSE -16

  // zgoščena vrednost SHA-256 z DER kodiranega QSealC končnega subjekta.
  // 32 bajtov, predstavljenih kot 64 hex znakov.
  "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

  },
  },

"unprotectedHeader": {}, // prazno v tem primeru

// podpis ES256 COSE: 64 bajtov = 128 hex znakov.
"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

```

## 9. Uporaba kriptografskih mehanizmov

Uporaba kriptografskih mehanizmov v okviru te priloge je skladna z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetско varnost in objavila Agencija Evropske unije za kibernetско varnost (ENISA).

### **PRILOGA III**

#### **SPOROČANJE INFORMACIJ IZ ČLENA 6(2)**

1. Države članice Komisiji sporočijo naslednje informacije o vsakem pristojnem organu ali telesu, odgovornem za izdajo fizičnih različic evropske kartice ugodnosti za invalide in evropske parkirne karte za invalide:
  - (a) ime pristojnega organa ali telesa, odgovornega za izdajo fizičnih različic evropske kartice ugodnosti za invalide in evropske parkirne karte za invalide;
  - (b) registrsko številko pristojnega organa ali telesa, odgovornega za izdajo fizičnih različic evropske kartice ugodnosti za invalide in evropske parkirne karte za invalide;
  - (c) kontaktni e-naslov in kontaktno telefonsko številko pristojnega organa ali telesa, odgovornega za izdajo fizičnih različic evropske kartice ugodnosti za invalide in evropske parkirne karte za invalide;
  - (d) eno ali več potrdil, ki se lahko uporabijo za preverjanje elektronskega žiga, ki ga je ustvaril pristojni organ ali telo, odgovorno za izdajo fizične različice evropske kartice ugodnosti za invalide ali evropske parkirne karte za invalide, in za katere potrjeni podatki o identiteti vključujejo ime in registrsko številko izdajatelja, kot je določeno v točki (a) oziroma (b);
  - (e) URL mesta, na katerem izdajatelj objavlja status veljavnosti fizičnih različic evropske kartice ugodnosti za invalide ali evropske parkirne karte za invalide.
2. Države članice lahko Komisiji sporočijo naslednje informacije o vsakem pristojnem organu ali telesu, odgovornem za izdajo fizičnih različic evropske kartice ugodnosti za invalide in evropske parkirne karte za invalide:
  - (a) URL spletne strani, na kateri so navedeni politike in pogoji pristojnega organa ali telesa, odgovornega za izdajo fizične različice evropske kartice ugodnosti za invalide ali evropske parkirne karte za invalide, ki se uporabljajo za zagotavljanje in uporabo fizične različice evropske kartice ugodnosti za invalide in evropske parkirne karte za invalide, ki jo tak organ ali telo zagotavlja;
  - (b) po potrebi URL spletne strani, na kateri so dodatne informacije o pristojnem organu ali telesu, odgovornem za izdajo fizičnih različic evropske kartice ugodnosti za invalide in evropske parkirne karte za invalide.

## PRILOGA IV

### **TEHNIČNE SPECIFIKACIJE ZA SEZNAM PREKLICEV ZA FIZIČNO RAZLIČICO EVROPSKE KARTICE UGODNOSTI ZA INVALIDE ALI EVROPSKE PARKIRNE KARTE ZA INVALIDE**

1. Za namene te priloge identifikator ustreza identifikatorju preklica (RID), opredeljenemu v točki 6 Priloge I in točki 6 Priloge II.
2. Seznam preklicev se izvaja kot žeton seznama identifikatorjev v obliki CWT (RFC 8392, oddelek 7) v skladu s klavzulo 5.2 specifikacije seznama statusov žetonov (draft-ietf-oauth-status-list-14) z naslednjimi spremembami:
  - (a) vrednost trditve type je "application/identifierlist+cwt";
  - (b) navedena je trditev časa izteka veljavnosti;
  - (c) trditev StatusList ni navedena v naboru trditev CWT;
  - (d) struktura IdentifierList, opredeljena v točki 3, je kot trditev navedena v naboru zahtevkov CWT z uporabo ključa 65530;
  - (e) CWT je objekt COSE\_Sign1, ki za izračun podpisa uporablja algoritem podpisa, skladen z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila Agencija Evropske unije za kibernetsko varnost (ENISA);
  - (f) CWT v zaščiteni glavi vsebuje parameter x5chain, kot je opredeljen v RFC 9360 (oddelek 2) in ki vsebuje potrdilo ali verigo potrdil za preverjanje podpisa seznama preklicev;
  - (g) razširjena uporaba ključa OID iz specifikacije seznama statusov žetonov (draft-ietf-oauth-status-list-14) se lahko uporablja za potrdilo o podpisu seznama identifikatorjev, pri čemer je priporočljivo, da preveritelji podpirajo razširjeno uporabo ključa OID iz specifikacije seznama statusov žetonov in da infrastrukture organa izdajatelja ne določijo razširjenega polja uporabe ključa kot obveznega pri uporabi razširjene uporabe ključa OID iz specifikacije seznama statusov žetonov.
3. Struktura IdentifierList je struktura CBOR z naslednjim Concise Data Definition Language (CDDL):

```
IdentifierList = {  
  "identifiers" : { * Identifier => IdentifierInfo },  
  ? "aggregation_uri" : Aggregation_uri,  
  * tstr => RFU  
}
```

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

Identifier = bstr

Aggregation\_uri = tstr