Vijeće
Europske unije

Bruxelles, 10. srpnja 2026.
(OR. en)

11772/26
ADD 1

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

POPRATNA BILJEŠKA

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	1. srpnja 2026.
Za:	Thérèse BLANCHET, glavna tajnica Vijeća Europske unije
Br. dok. Kom.:	C(2026) 4534 annex
Predmet:	PRILOZI DELEGIRANOJ UREDBI KOMISIJE (EU) .../... o dopuni Direktive (EU) 2024/2841 u pogledu uspostave QR koda za fizičku verziju europske iskaznice za osobe s invaliditetom, uspostave QR koda i utvrđivanja zajedničkih tehničkih specifikacija kojima se osigurava sigurnost fizičke verzije europske parkirališne karte za osobe s invaliditetom te pitanja interoperabilnosti

EUROPSKA
KOMISIJA

Bruxelles, 1.7.2026.
C(2026) 4534 final

ANNEXES 1 to 4

PRILOZI

DELEGIRANOJ UREDBI KOMISIJE (EU) .../...

o dopuni Direktive (EU) 2024/2841 u pogledu uspostave QR koda za fizičku verziju europske iskaznice za osobe s invaliditetom, uspostave QR koda i utvrđivanja zajedničkih tehničkih specifikacija kojima se osigurava sigurnost fizičke verzije europske parkirališne karte za osobe s invaliditetom te pitanja interoperabilnosti

PRILOG I.

SPECIFIKACIJE ZA QR KOD NA FIZIČKOJ VERZIJI EUROPSKE ISKAZNICE ZA OSOBE S INVALIDITETOM

1. **Format QR koda za fizičku verziju europske iskaznice za osobe s invaliditetom**

(a) **Format QR koda model 2** u skladu s međunarodnim specifikacijama za QR kodove ISO/IEC 18004:2024 ili jednakovrijednim specifikacijama.

(b) **Razina ispravljanja pogrešaka M** (rekonstrukcija 15 % zapisa) kojom se osigurava otpornost na ogrebotine ili djelomično oštećenje tiskanog QR koda.

(c) **Način kodiranja:** Korisni sadržaj QR koda sastoji se od kombinirane issuerSigned Concise Binary Object Representation (CBOR) strukture i odgovarajućeg issuerAuth COSE_Sign1 objekta potpisa kako je definirano u specifikaciji za COSE (CBOR Object Signing and Encryption) (RFC 9052, odjeljci 3.1., 4.2. i 4.4.), u skladu s obrascem podatkovnog modela mDOC za stavke koje je potpisao izdavatelj (issuerSigned items), ali prilagođeno za fiksne fizičke isprave. IssuerAuth je COSE_Sign1 objekt s alg = ES256 i zaštićenim zaglavljem koje sadržava x5t (hash parametar zaglavlja certifikata COSE X.509 definiran u dokumentu RFC 9360 (odjeljak 2.); za potrebe interoperabilnosti hash algoritam koji se upotrebljava u x5t je SHA-256).

(d) Prije kodiranja QR koda kombinirani CBOR/COSE objekt **komprimira se u formatu zlib** (RFC 1950, odjeljak 2.2.) pomoću algoritma **deflate** (RFC 1951, odjeljci 3.2. i 4.). Dobiveno komprimirano polje bajtova kodira se u **QR kod u formatu Byte Mode** (kodiranje u bajtovima), čime se u potpunosti podržava interoperabilnost binarnog CBOR/COSE korisnog sadržaja i skenera.

Za sva polja za unos teksta uključena u korisni sadržaj QR koda izdavatelji znakove kodiraju prema standardu Unicode UTF-8 unutar CBOR znakovnih nizova. Transliteracija se ne primjenjuje na potpisane podatke u korisnom sadržaju. Za potrebe interoperabilnosti izdavatelji prije potpisivanja na sva polja s tekstualnim podacima primjenjuju standard Unicode Normalisation Form C (NFC).

(e) **Prefiks:** QR niz europske iskaznice za osobe s invaliditetom započinje s „ED1:MDOC:”. Time se identificiraju vrsta isprave i profil kodiranja. Prefiksi su osjetljivi na velika i mala slova i moraju biti prisutni. Nepoznati ili nepodržani prefiksi dovode do odbijanja. Prefiks i komprimirani korisni sadržaj kodiraju se u QR kod kao jedinstveni podatkovni segment u formatu Byte Mode.

(f) **Najmanja veličina modula ≥ 0,25 mm** kako bi se osigurala čitljivost na tiskanim iskaznicama.

(g) **Najveća verzija je verzija 20;** s najviše 97 × 97 modula na svakoj strani.

2. **Specifikacije za generiranje potpisa za europsku iskaznicu za osobe s invaliditetom**

Kvalificiranim elektroničkim pečatom (QSeal) koji se upotrebljava za pečaćenje QR kodova na europskim iskaznicama za osobe s invaliditetom jamči se da kodirani podaci potječu od ovlaštenog izdavatelja i da nisu izmijenjeni.

(a) **Algoritam potpisa**: Algoritam potpisa je ES256 (algoritam za digitalno potpisivanje zasnovan na eliptičnim krivuljama (ECDSA) koji je kombinacija algoritma SHA-256 i krivulje P-256), kako je definiran u dokumentu RFC 9053 (odjeljak 2.1.); u COSE-u algoritam se identificira prema parametru alg zaglavlja iz dokumenta RFC 9052 (odjeljak 3.1.).

(b) **Potpisni ključ**: Korisni sadržaj QR koda potpisuje se privatnim ključem koji odgovara kvalificiranom certifikatu za elektronički pečat (QSealC).

(c) **COSE struktura:** Spremnik potpisa je COSE_Sign1 objekt. Zaštićeno zaglavlje uključuje alg (ES256) i x5t (hash parametar zaglavlja certifikata COSE X.509 definiran u dokumentu RFC 9360 (odjeljak 2.); za potrebe interoperabilnosti hash algoritam koji se upotrebljava u x5t je SHA-256). Provjera se oslanja na korištenje x5t vrijednosti za pronalazak odgovarajućeg certifikata u lokalno cachiranom spremištu pouzdanih certifikata vršitelja provjera (*trust store*) koje se sastoji od informacija s popisa pouzdanih subjekata, a zatim se lanac certifikata i status certifikata validiraju u skladu s okvirom povjerenja eIDAS-a.

(d) **Standard potpisa**: Korisni sadržaj QR koda potpisuje se kao COSE_Sign1 objekt u skladu s RFC 9052 (odjeljak 4.), COSE (CBOR Object Signing and Encryption). COSE_Sign1 objekt provodi se u issuerAuth i kodira bez oznake CBOR za COSE_Sign1. Polje korisnog sadržaja COSE_Sign1 objekta odvaja se i kodira kao CBOR null. Za generiranje i provjeru potpisa vanjski korisni sadržaj je deterministička CBOR kodirana struktura koja sadržava vrijednost docType i vrijednost issuerSigned iz CBOR mape najviše razine.

(e) **Hash algoritam**: SHA-256 koristi se kao dio algoritma ES256 za generiranje potpisa i provjeru cjelovitosti.

(f) **Kodiranje**: Korisni sadržaj kodira se pomoću CBOR-a (RFC 8949, odjeljak 4.2.), kako je propisano specifikacijama za COSE i mDOC, čime se omogućuju kodiranje i reproduciranje potpisanih podataka.

3. **Specifikacije tiskanja isprave**

(a) **Prazan prostor**: Prazan prostor od **četiri modula** mora okruživati QR kod sa svih strana, bez ikakvog tiska, uzorka ili pozadine.

(b) **Kontrast**: QR kod mora biti otisnut na bijeloj pozadini s minimalnim omjerom kontrasta **4:1** kako bi bio jasno čitljiv u različitim uvjetima osvjetljenja.

(c) QR kod se tiska bojom definiranom u Prilogu I. Direktivi (EU) 2024/2841, čime se postiže najveći kontrast.

(d) **Smještaj i veličina**: QR kod, uključujući prazan prostor oko njega, mora imati dimenzije 26,25 mm × 26,25 mm i smješten u donjem desnom kutu poleđine iskaznice. Najveća verzija QR koda može biti verzija 20 (97 × 97 modula), s modulom veličine 0,25 mm ili više.

QR kod, uključujući prazan prostor oko njega, mora biti najmanje 5 mm od desnog ruba i najmanje 5 mm od donjeg ruba iskaznice.

4. **Podaci u QR kodu europske iskaznice za osobe s invaliditetom**

QR kod sadržava minimalan skup podataka koji se može provjeriti izvan interneta u skladu s načelom smanjenja količine podataka iz članka 5. stavka 1. točke (c) Uredbe (EU) 2016/679. Struktura korisnog sadržaja je sljedeća:

(a) Atributi iskaznice kodiraju se u CBOR-u unutar objekta issuerSigned.

(b) Struktura je zapakirana i potpisana koristeći QSeal izdavatelja kao issuerAuth (COSE_Sign1, ES256, uključujući x5t, hash parametar zaglavlja certifikata COSE X.509).

(c) Dobiveni CBOR/COSE objekt komprimira se u skladu s točkom 1. podtočkom (d) ovog Priloga. Korisni sadržaj QR koda sastoji se od prefiksa „ED1:MDOC:", nakon kojeg slijedi dobiveno komprimirano polje bajtova, a cijeli korisni sadržaj kodira se kao jedinstveni podatkovni segment QR koda u formatu Byte Mode.

Sadržaj podataka sastoji se od podskupa vidljivih podataka iz polja na prednjoj strani iskaznice navedenih u Prilogu I. Direktivi (EU) 2024/2841 (ime, prezime, serijski broj iskaznice, datum isteka), zajedno s identifikatorom opoziva, elektroničkim potpisom i informacijama o shemi.

Elektronički potpis sadržava:

i. issuerAuth – COSE_Sign1 objekt potpisan **privatnim ključem QSealC** izdavatelja;

ii. zaštićeno zaglavlje koje uključuje alg = ES256 (algoritam potpisa) i x5t (hash parametar zaglavlja certifikata COSE X.509).

5. Neobvezni podaci

QR kod ne sadržava neobvezne podatke.

6. Identifikator opoziva

Uz vidljiv serijski broj iskaznice QR kod uključuje i poseban identifikator opoziva.

Identifikator opoziva upotrebljava se za utvrđivanje statusa opoziva i za upravljanje popisom opozvanih isprava. Identifikator opoziva ne tiska se na iskaznici i ne prikazuje vršiteljima provjera isprava.

6.1. *Zahtjevi za identifikator opoziva*

Identifikator opoziva:

(a) uključen je u potpisani korisni sadržaj QR koda;

(b) jedinstven je barem u području u nadležnosti tijela koje izdaje iskaznicu;

(c) ne tiska se na iskaznici i nije čitljiv ljudima;

(d) ne otkriva osobne podatke i nije izravno razumljiv;

(e) nije izravno izveden iz vidljivog serijskog broja iskaznice; i

(f) kriptografski se veže uz korisni sadržaj QR koda kvalificiranim elektroničkim pečatom.

6.2. *Format i veličina identifikatora opoziva*

Identifikator opoziva kodira se kao CBOR niz bajtova (bstr). Identifikator opoziva ima 16 bajtova (128 bita).

Tijelo izdavatelj generira identifikator opoziva koristeći metodu unutar svoje kontrole kojom se osiguravaju dovoljna entropija i otpornost na pogađanje ili nabrajanje.

6.3. *Popisi opozvanih isprava*

U popisima opozvanih isprava koji se objavljuju za potrebe provjere upućuje se samo na identifikator opoziva opozvanih isprava. Objavljeni popisi opozvanih isprava ne sadržavaju serijske brojeve iskaznica.

7. CBOR korisni sadržaj (unutar QR koda) europske iskaznice za osobe s invaliditetom

U korisni sadržaj QR koda uključuju se samo sljedeći podaci, u skladu s vidljivim podatkovnim poljima na europskoj iskaznici za osobe s invaliditetom iz Priloga I. Direktivi (EU) 2024/2841.

Sadržaj na najvišoj razini:

(a) docType = "eu.edc";

(b) issuerSigned.nameSpaces."eu.edc" s atributima prikazanima u tablici u nastavku;

(c) issuerAuth = COSE_Sign1 (QSeal).

Polje	**mDOC putanja**	**Vrsta/format**
Verzija podatkovne sheme	issuerSigned.nameSpaces."eu.edc".ver	Niz (npr. "1.0")
Vrsta isprave: europska iskaznica za osobe s invaliditetom	docType	Enum ("eu.edc")
Serijski broj iskaznice	issuerSigned.nameSpaces."eu.edc".sub	Niz
Identifikator opoziva	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bajtova)
Ime nositelja iskaznice	issuerSigned.nameSpaces."eu.edc".givenName	Tekstni niz prema standardu Unicode (UTF-8)
Prezime nositelja iskaznice	issuerSigned.nameSpaces."eu.edc".familyName	Tekstni niz prema standardu Unicode (UTF-8)

Datum isteka iskaznice	issuerSigned.nameSpaces."eu.edc".exp	Oznaka CBOR 1004, kako je definirana u RFC 8943 (odjeljak 2.1.), koja sadržava tekstni niz kodiran u UTF-8 čiji je sadržaj puni datum prema RFC 3339 u formatu GGGG-MM-DD.

Elektronički potpis provodi se u issuerAuth (COSE_Sign1 objekt). Lanac certifikata ne smije biti ugrađen u korisni sadržaj QR koda; umjesto toga, zaštićeno COSE zaglavlje mora sadržavati x5t, digitalni otisak certifikata za lociranje odgovarajućeg QSealC u kopiji spremišta pouzdanih certifikata (*cached trust store*) vršitelja provjera.

8. **Primjer korisnog sadržaja QR koda na europskoj iskaznici za osobe s invaliditetom: komentirani logički prikaz u formatu koji odgovara JSON-u (JavaScript Object Notation)**

Ovo je primjer logičkog prikaza europske iskaznice za osobe s invaliditetom u JSON-u koji je čitljiv ljudima. U praksi ta struktura neće biti čitljiva ljudima jer:

(a) biti kodirana u CBOR-u (RFC 8949, odjeljak 3.);

(b) biti potpisana neoznačenom strukturom COSE_Sign1 s odvojenim korisnim sadržajem (RFC 9052, odjeljak 4.);

(c) uključivati datum isteka kao oznaku CBOR 1004 s vrijednošću za puni datum u skladu s RFC 8943 (odjeljak 2.1.);

(d) uključivati parametar x5t zaštićenog zaglavlja u skladu s RFC 9360, koristeći SHA-256 preko QSealC krajnjeg subjekta kodiranog DER kodom; i

(e) biti komprimirana i kao prefiks sadržavati niz ED1:MDOC: prije kodiranja u QR kod.

```
{
  // u skladu s JSON-om, samo logički prikaz europske iskaznice za osobe s invaliditetom koji je čitljiv ljudima.
  // stvarni korisni sadržaj QR koda je deterministički CBOR, a ne JSON.
  "docType": „eu.edc”, // vjerodajnica europske iskaznice za osobe s invaliditetom. Uključena je vrijednost docType, zajedno s
    //issuerSigned, u vanjskom korisnom sadržaju COSE_Sign1.

  "issuerSigned": {
    // Podaci zaštićeni s issuerAuth; ovdje su oni odvojeni korisni sadržaj.
    // Za generiranje i provjeru potpisa odvojen vanjski korisni sadržaj obuhvaća i
    // docType i issuerSigned.
    "nameSpaces": {
      "eu.edc": {
        "ver": "1.0", // verzija profila/sheme QR koda

        // Serijski broj iskaznice; prema definiciji izdavatelja, najviše 24 znaka.
        "sub": "AB123456789012345678 90CD",
```

```
      // Identifikator opoziva: stvarni CBOR bstr, 16 bajtova/128 bitova.
      // Ovdje prikazano s 32 heksadecimalna znaka radi čitljivosti.
      "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      "givenName": "Ivo",    // ime otisnuto na europskoj iskaznici za osobe s invaliditetom
      "familyName": "Ivić", // prezime otisnuto na europskoj iskaznici za osobe s
invaliditetom

      // Stvarno kodiranje CBOR koristi oznaku 1004 za puni datum prema RFC 3339.
      "exp": "2030-12-31"
    }
  }
},

 "issuerAuth": {
  // Stvarni oblik: neoznačeni COSE_Sign1, ne JSON objekt.
  „type”: "COSE_Sign1",
  "tagged": false,       // kodirano bez CBOR oznake COSE_Sign1 CBOR
  "payload": "detached", // polje korisnog sadržaja COSE je CBOR null

  "protectedHeader": {
   // alg: ES256; ekvivalentni parametar zaglavlja COSE 1 = -7.
   "alg": "ES256",

   // x5t: digitalni otisak certifikata; parametar zaglavlja COSE 34.
   "x5t": {
    "hashAlg": "SHA-256", // ekvivalentni COSE hash -16
```

```
        // SHA-256 hash za QSealC krajnji subjekt kodiran DER kodom;
        // 32 bajta prikazana sa 64 heksadecimalna znaka.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // u ovom primjeru prazno

    // ES256 COSE potpis: 64 bajta = 128 heksadecimalnih znakova.
    "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```


9. Korištenje kriptografskih mehanizama

Korištenje kriptografskih mehanizama u kontekstu ovog Priloga mora biti u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila Agencija Europske unije za kibersigurnost (ENISA).

PRILOG II.

SPECIFIKACIJE ZA QR KOD NA FIZIČKOJ VERZIJI EUROPSKE PARKIRALIŠNE KARTE ZA OSOBE S INVALIDITETOM

1. **Format QR koda za fizičku verziju europske parkirališne karte za osobe s invaliditetom**

(a) **Format QR koda model 2** u skladu s međunarodnim specifikacijama za QR kodove ISO/IEC 18004:2024 ili jednakovrijednim specifikacijama.

(b) **Razina ispravljanja pogrešaka M** (rekonstrukcija 15 % zapisa) kojom se osigurava otpornost na ogrebotine ili djelomično oštećenje tiskanog QR koda.

(c) **Način kodiranja:** Korisni sadržaj QR koda sastoji se od kombinirane issuerSigned Concise Binary Object Representation (CBOR) strukture i odgovarajućeg issuerAuth COSE_Sign1 objekta potpisa kako je definirano u specifikaciji za COSE (CBOR Object Signing and Encryption) (RFC 9052, odjeljci 3.1., 4.2. i 4.4.), u skladu s obrascem podatkovnog modela mDOC za stavke koje je potpisao izdavatelj (issuerSigned items), ali prilagođeno za fiksne fizičke isprave. IssuerAuth je COSE_Sign1 objekt s alg = ES256 i zaštićenim zaglavljem koje sadržava x5t (hash parametar zaglavlja certifikata COSE X.509 definiran u RFC 9360 (odjeljak 2.); za potrebe interoperabilnosti hash algoritam koji se upotrebljava u x5t je SHA-256).

(d) Prije kodiranja QR koda kombinirani CBOR/COSE objekt **komprimira se u formatu zlib (RFC 1950, odjeljak 2.2.)** pomoću algoritma **deflate** (RFC 1951, odjeljci 3.2. i 4.). Dobiveno komprimirano polje bajtova kodira se u **QR kod u formatu Byte Mode** (kodiranje u bajtovima), čime se u potpunosti podržava interoperabilnost binarnog CBOR/COSE korisnog sadržaja i skenera.

Za sva polja za unos teksta uključena u korisni sadržaj QR koda izdavatelji znakove kodiraju prema standardu Unicode UTF-8 unutar CBOR znakovnih nizova. Transliteracija se ne primjenjuje na potpisane podatke u korisnom sadržaju. Za potrebe interoperabilnosti izdavatelji prije potpisivanja na sva polja s tekstualnim podacima primjenjuju standard Unicode Normalisation Form C (NFC).

(e) **Prefiks**: QR niz europske parkirališne karte za osobe s invaliditetom započinje s „EP1:MDOC:”. Time se identificiraju vrsta isprave i profil kodiranja. Prefiksi su osjetljivi na velika i mala slova i moraju biti prisutni. Nepoznati ili nepodržani prefiksi dovode do odbijanja. Prefiks i komprimirani korisni sadržaj kodiraju se u QR kod kao jedinstveni podatkovni segment u formatu Byte Mode.

(f) **Najmanja veličina modula ≥ 0,35 mm** kako bi se osigurala čitljivost na tiskanim kartama.

(g) **Najveća verzija je verzija 20**; s najviše 97 × 97 modula na svakoj strani.

2. **Specifikacije za generiranje potpisa za europsku parkirališnu kartu za osobe s invaliditetom**

Kvalificiranim elektroničkim pečatom (QSeal) koji se upotrebljava za pečaćenje QR kodova na europskim parkirališnim kartama za osobe s invaliditetom jamči se da kodirani podaci potječu od ovlaštenog izdavatelja i da nisu izmijenjeni.

(a) **Algoritam potpisa**: Algoritam potpisa je ES256 (ECDSA koji je kombinacija algoritma SHA-256 i krivulje P-256), kako je definirano u dokumentu RFC 9053

(odjeljak 2.1.); u COSE-u algoritam se identificira prema parametru alg zaglavlja iz dokumenta RFC 9052 (odjeljak 3.1.).

(b) **Potpisni ključ**: Korisni sadržaj QR koda potpisuje se privatnim ključem koji odgovara kvalificiranom certifikatu za elektronički pečat (QSealC).

(c) **COSE struktura**: Spremnik potpisa je COSE_Sign1 objekt. Zaštićeno zaglavlje uključuje alg (ES256) i x5t (hash parametar zaglavlja certifikata COSE X.509 definiran u dokumentu RFC 9360 (odjeljak 2.); za potrebe interoperabilnosti hash algoritam koji se upotrebljava u x5t je SHA-256). Provjera se oslanja na korištenje x5t vrijednosti za pronalazak odgovarajućeg certifikata u lokalno cachiranom spremištu pouzdanih certifikata vršitelja provjera (*trust store*) koje se sastoji od informacija s popisa pouzdanih subjekata, a zatim se lanac certifikata i status certifikata validiraju u skladu s okvirom povjerenja eIDAS-a.

(d) **Standard potpisa**: Korisni sadržaj QR koda potpisuje se kao COSE_Sign1 objekt u skladu s RFC 9052 (odjeljak 4.), COSE (CBOR Object Signing and Encryption). COSE_Sign1 objekt provodi se u issuerAuth i kodira bez oznake CBOR za COSE_Sign1. Polje korisnog sadržaja COSE_Sign1 objekta odvaja se i kodira kao CBOR null. Za generiranje i provjeru potpisa vanjski korisni sadržaj je deterministička CBOR kodirana CBOR struktura koja sadržava vrijednost docType i vrijednost issuerSigned iz CBOR mape najviše razine.

(e) **Hash algoritam**: SHA-256 koristi se kao dio algoritma ES256 za generiranje potpisa i provjeru cjelovitosti.

(f) **Kodiranje**: Korisni sadržaj kodira se pomoću CBOR-a (RFC 8949, odjeljak 4.2.), kako je propisano specifikacijama za COSE i mDOC, čime se omogućuju kodiranje i reproduciranje potpisanih podataka.

3. **Specifikacije tiskanja isprave**

(a) **Prazan prostor**: Prazan prostor od **četiri modula** mora okruživati QR kod sa svih strana, bez ikakvog tiska, uzorka ili pozadine.

(b) **Kontrast**: QR kod mora biti otisnut na bijeloj pozadini s minimalnim omjerom kontrasta **4:1** kako bi bio jasno čitljiv u različitim uvjetima osvjetljenja.

(c) QR kod se tiska bojom definiranom u Prilogu II. Direktivi (EU) 2024/2841, čime se postiže najveći kontrast.

(d) **Smještaj i veličina:** QR kod, uključujući prazan prostor oko njega, ima dimenzije **37 mm × 37 mm** i nalazi se na prednjoj strani karte, blago desno od centra, prema donjem rubu. Najveća verzija QR koda može biti verzija 20 (97 × 97 modula), s modulom veličine 0,35 mm ili više.

QR kod, uključujući prazan prostor oko njega, mora biti najmanje 5 mm od donjeg ruba karte.

4. **Podaci u QR kodu europske parkirališne karte za osobe s invaliditetom**

QR kod sadržava minimalan skup podataka koji se može provjeriti izvan interneta u skladu s načelom smanjenja količine podataka iz članka 5. stavka 1. točke (c) Uredbe (EU) 2016/679. Struktura korisnog sadržaja je sljedeća:

(a) Atributi karte kodiraju se u CBOR-u unutar objekta issuerSigned.

(b) Struktura je zapakirana i potpisana koristeći QSeal izdavatelja kao issuerAuth (COSE_Sign1, ES256, uključujući x5t, hash parametar zaglavlja certifikata COSE X.509).

(c) Dobiveni CBOR/COSE objekt komprimira se u skladu s točkom 1. podtočkom (d) ovog Priloga. Korisni sadržaj QR koda sastoji se od prefiksa „EP1:MDOC:”, nakon kojeg slijedi dobiveno komprimirano polje bajtova, a cijeli korisni sadržaj kodira se kao jedinstveni podatkovni segment QR koda u formatu Byte Mode.

Sadržaj podataka sastoji se od podskupa vidljivih podataka iz polja na prednjoj strani karte navedenih u Prilogu II. Direktivi (EU) 2024/2841 (datum isteka, serijski broj karte), zajedno s identifikatorom opoziva, elektroničkim potpisom i informacijama o shemi.

Elektronički potpis sadržava:

i. issuerAuth – COSE_Sign1 objekt potpisan **privatnim ključem QSealC** izdavatelja;

ii. zaštićeno zaglavlje koje uključuje alg = ES256 (algoritam potpisa) i x5t (hash parametar zaglavlja certifikata COSE X.509).

5. Neobvezni podaci

QR kod ne sadržava neobvezne podatke.

6. Identifikator opoziva

Identifikator opoziva europske parkirališne karte za osobe s invaliditetom mora biti u skladu s točkom 6. Priloga I.

U popisima opozvanih europskih parkirališnih karata za osobe s invaliditetom upućuje se samo na identifikator opoziva. Objavljeni popisi opozvanih isprava ne sadržavaju serijske brojeve karata.

7. CBOR korisni sadržaj (unutar QR koda) europske parkirališne karte za osobe s invaliditetom

U korisni sadržaj QR koda uključuju se samo sljedeći podaci, u skladu s vidljivim podatkovnim poljima na europskoj parkirališnoj karti za osobe s invaliditetom iz Priloga II. Direktivi (EU) 2024/2841:

Polje	**mDOC putanja**	**Vrsta/format**
Verzija podatkovne sheme	issuerSigned.nameSpaces."eu.epc".ver	Niz (npr. "1.0")
Vrsta isprave: europska parkirališna karta za osobe s invaliditetom	docType	Enum ("eu.epc")
Serijski broj	issuerSigned.nameSpaces."eu.epc".sub	Niz

karte		
Identifikator opoziva	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 bajtova)
Datum isteka karte	issuerSigned.nameSpaces."eu.epc".exp	Oznaka CBOR 1004, kako je definirana u RFC 8943 (odjeljak 2.1.), koja sadržava tekstni niz kodiran u UTF-8 čiji je sadržaj puni datum prema RFC 3339 u formatu GGGG-MM-DD.

Elektronički potpis provodi se u issuerAuth (COSE_Sign1 objekt). Lanac certifikata ne smije biti ugrađen u korisni sadržaj QR koda; umjesto toga, zaštićeno COSE zaglavlje mora sadržavati x5t, digitalni otisak certifikata za lociranje odgovarajućeg QSealC u kopiji spremišta pouzdanih certifikata (*cached trust store*) vršitelja provjera.

8. Primjer korisnog sadržaja QR koda na europskoj parkirališnoj karti za osobe s invaliditetom komentirani logički prikaz u formatu koji odgovara JSON-u (JavaScript Object Notation)

Ovo je primjer logičkog prikaza europske parkirališne karte za osobe s invaliditetom u JSON-u koji je čitljiv ljudima. U praksi ta struktura neće biti čitljiva ljudima jer mora:

(a) biti kodirana u CBOR-u (RFC 8949, odjeljak 3.);

(b) biti potpisana neoznačenom strukturom COSE_Sign1 s odvojenim korisnim sadržajem (RFC 9052, odjeljak 4.);

(c) uključivati datum isteka kao oznaku CBOR 1004 s vrijednošću za puni datum u skladu s RFC 8943 (odjeljak 2.1.);

(d) uključivati parametar x5t zaštićenog zaglavlja u skladu s RFC 9360, koristeći SHA-256 preko QSealC krajnjeg subjekta kodiranog DER kodom; i

(e) biti komprimirana i kao prefiks sadržavati niz EP1:MDOC: prije kodiranja u QR kod.

{

```
  // u skladu s JSON-om, samo logički prikaz europske parkirališne karte za osobe s invaliditetom koji je čitljiv ljudima.

  // stvarni korisni sadržaj QR koda je deterministički CBOR, a ne JSON.

  "docType": "eu.epc", // vjerodajnica europske parkirališne karte za osobe s invaliditetom. Uključena je vrijednost docType, zajedno s

    //issuerSigned, u vanjskom korisnom sadržaju COSE_Sign1.


  "issuerSigned": {

    // Podaci zaštićeni s issuerAuth; ovdje su oni odvojeni korisni sadržaj.

 // Za generiranje i provjeru potpisa odvojen vanjski korisni sadržaj obuhvaća i

    // docType i issuerSigned.

    "nameSpaces": {

      "eu.epc": {

        "ver": "1.0", // verzija profila/sheme QR koda


        // Serijski broj iskaznice; prema definiciji izdavatelja, najviše 24 znaka.

        "sub": "EF123456789012345678 90GH",


        // Identifikator opoziva: stvarni CBOR bstr, 16 bajtova/128 bitova.

        // Ovdje prikazano s 32 heksadecimalna znaka radi čitljivosti.

        "rid": "4a8d9c112233445566778899aabbccdd",


        // Stvarno kodiranje CBOR koristi oznaku 1004 za puni datum prema RFC 3339.

        "exp": "2030-12-31"

      }

    }

  },
```

```
 "issuerAuth": {
  // Stvarni oblik: neoznačeni COSE_Sign1, ne JSON objekt.
  „type”: "COSE_Sign1",
  "tagged": false,       // kodirano bez CBOR oznake COSE_Sign1 CBOR
  "payload": "detached", // polje korisnog sadržaja COSE je CBOR null

  "protectedHeader": {
   // alg: ES256; ekvivalentni parametar zaglavlja COSE 1 = -7.
   "alg": "ES256",

   // x5t: digitalni otisak certifikata; parametar zaglavlja COSE 34.
   "x5t": {
    "hashAlg": "SHA-256", // ekvivalentni COSE hash -16

    // SHA-256 hash za QSealC krajnji subjekt kodiran DER kodom;
    // 32 bajta prikazana sa 64 heksadecimalna znaka.
    "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
   }
  },

  "unprotectedHeader": {}, // u ovom primjeru prazno

  // ES256 COSE potpis: 64 bajta = 128 heksadecimalnih znakova.
  "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
 }
```

}

9. Korištenje kriptografskih mehanizama

Korištenje kriptografskih mehanizama u kontekstu ovog Priloga mora biti u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila Agencija Europske unije za kibersigurnost (ENISA).

PRILOG III.

DOSTAVLJANJE INFORMACIJA IZ ČLANKA 6. STAVKA 2.

1. Države članice Komisiji dostavljaju sljedeće informacije o svakom nadležnom tijelu ili tijelu odgovornom za izdavanje fizičkih verzija europske iskaznice za osobe s invaliditetom ili europske parkirališne karte za osobe s invaliditetom:

   (a) naziv nadležnog tijela ili tijela odgovornog za izdavanje fizičkih verzija europske iskaznice za osobe s invaliditetom ili europske parkirališne karte za osobe s invaliditetom;

   (b) registracijski broj nadležnog tijela ili tijela odgovornog za izdavanje fizičkih verzija europske iskaznice za osobe s invaliditetom ili europske parkirališne karte za osobe s invaliditetom;

   (c) e-adresu i telefonski broj za kontakt nadležnog tijela ili tijela odgovornog za izdavanje fizičkih verzija europske iskaznice za osobe s invaliditetom ili europske parkirališne karte za osobe s invaliditetom;

   (d) jedan ili više certifikata koji se mogu koristiti za provjeru elektroničkog pečata koji je nadležno tijelo ili tijelo odgovorno za izdavanje fizičkih verzija europske iskaznice za osobe s invaliditetom ili europske parkirališne karte za osobe s invaliditetom izradilo za isprave koje izdaje, pri čemu certificirani podaci o identitetu trebaju obuhvaćati ime i registracijski broj izdavatelja iz točke (a) odnosno točke (b);

   (e) URL lokacije na kojoj izdavatelj objavljuje status valjanosti fizičkih verzija europske iskaznice za osobe s invaliditetom ili europske parkirališne karte za osobe s invaliditetom.

2. Države članice Komisiji mogu dostaviti sljedeće informacije o svakom nadležnom tijelu ili tijelu odgovornom za izdavanje fizičkih verzija europske iskaznice za osobe s invaliditetom ili europske parkirališne karte za osobe s invaliditetom:

   (a) URL internetske stranice koja sadržava politike i uvjete nadležnog tijela ili tijela odgovornog za izdavanje fizičkih verzija europske iskaznice za osobe s invaliditetom ili europske parkirališne karte za osobe s invaliditetom koji se primjenjuju na izdavanje i upotrebu fizičkih verzija europske iskaznice za osobe s invaliditetom i europske parkirališne karte za osobe s invaliditetom koje ono izdaje;

   (b) ako je primjenjivo, URL internetske stranice koja sadržava dodatne informacije o nadležnom tijelu ili tijelu odgovornom za izdavanje fizičkih verzija europske iskaznice za osobe s invaliditetom ili europske parkirališne karte za osobe s invaliditetom.

PRILOG IV.

TEHNIČKE SPECIFIKACIJE ZA POPIS OPOZVANIH FIZIČKIH VERZIJA EUROPSKE ISKAZNICE ZA OSOBE S INVALIDITETOM ILI EUROPSKE PARKIRALIŠNE KARTE ZA OSOBE S INVALIDITETOM

1. Za potrebe ovog Priloga identifikator odgovara identifikatoru opoziva iz točke 6. Priloga I. i točke 6. Priloga II.

2. Popis opozvanih isprava koristi se kao token popisa identifikatora u formatu CWT (RFC 8392, odjeljak 7.) u skladu s klauzulom 5.2. specifikacije za popis statusa tokena (draft-ietf-oauth-status-list-14) sa sljedećim izmjenama:

   (a) vrijednost tvrdnje tipa mora biti „application/identifierlist+cwt”;

   (b) mora se navesti tvrdnja o isteku;

   (c) tvrdnja StatusList ne smije biti prisutna u CWT tvrdnjama;

   (d) struktura IdentifierList iz točke 3. mora biti prisutna kao tvrdnja u CWT tvrdnjama korištenjem ključa 65530;

   (e) CWT je COSE_Sign1 objekt koji za izračun potpisa upotrebljava algoritam potpisa u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila Agencija Europske unije za kibersigurnost (ENISA);

   (f) CWT sadržava parametar x5chain kako je definiran u dokumentu RFC 9360 (odjeljak 2.) u zaštićenom zaglavlju koje sadržava certifikat ili lanac certifikata za provjeru potpisa na popisu opozvanih isprava;

   (g) OID proširene upotrebe ključa iz specifikacije za popis statusa tokena (draft-ietf-oauth-status-list-14) može se upotrebljavati u certifikatu za potpisivanje popisa identifikatora te se preporučuje da vršitelji provjera podržavaju OID proširene upotrebe ključa iz specifikacije za popis statusa tokena i da infrastrukture izdavatelja ne postavljaju polje proširene upotrebe ključa kao kritično pri korištenju OID-a proširene upotrebe ključa iz specifikacije za popis statusa tokena.

3. Struktura IdentifierList je CBOR struktura sa sljedećim prikazom u CDDL-u (Concise Data Definition Language):

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

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

Identifier = bstr

Aggregation_uri = tstr