Rada
Európskej únie

V Bruseli 10. júla 2026
(OR. en)

11772/26
ADD 1

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

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	1. júla 2026
Komu:	Thérèse BLANCHETOVÁ, generálna tajomníčka Rady Európskej únie
Č. dok. Kom.:	C(2026) 4534 annex
Predmet:	PRÍLOHY k DELEGOVANÉMU NARIADENIU KOMISIE (EÚ) .../..., ktorým sa dopĺňa smernica (EÚ) 2024/2841, pokiaľ ide o stanovenie QR kódu na fyzickej verzii európskeho preukazu osoby so zdravotným postihnutím, stanovenie QR kódu a spoločných technických špecifikácií na zaistenie bezpečnosti fyzickej verzie európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím, ako aj prvkov interoperability

EURÓPSKA
KOMISIA

V Bruseli 1. 7. 2026
C(2026) 4534 final

ANNEXES 1 to 4

PRÍLOHY

k

DELEGOVANÉMU NARIADENIU KOMISIE (EÚ) .../...,

ktorým sa dopĺňa smernica (EÚ) 2024/2841, pokiaľ ide o stanovenie QR kódu na fyzickej verzii európskeho preukazu osoby so zdravotným postihnutím, stanovenie QR kódu a spoločných technických špecifikácií na zaistenie bezpečnosti fyzickej verzie európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím, ako aj prvkov interoperability

PRÍLOHA I

ŠPECIFIKÁCIE QR KÓDU PRE FYZICKÚ VERZIU EURÓPSKEHO PREUKAZU OSOBY SO ZDRAVOTNÝM POSTIHNUTÍM

1. **Formát QR kódu pre fyzickú verziu európskeho preukazu osoby so zdravotným postihnutím**

a) **Formát QR code Model 2** v súlade s medzinárodnými špecifikáciami pre QR kódy ISO/IEC 18004:2024 alebo rovnocennými špecifikáciami.

b) **Úroveň korekcie chýb M** (redundancia 15 %) zabezpečujúca odolnosť vytlačeného QR kódu voči škrabancom alebo voči čiastočnému poškodeniu.

c) **Režim kódovania:** Dátový obsah QR kódu pozostáva z kombinovanej štruktúry issuerSigned Concise Binary Object Representation (CBOR) a zodpovedajúceho objektu podpisu issuerAuth COSE_Sign1 v zmysle vymedzenia v CBOR Object Signing and Encryption (COSE, RFC 9052 oddiely 3.1, 4.2 a 4.4) a zodpovedá vzoru modelu údajov mDOC pre položky issuerSigned, ale prispôsobenému na používanie na statických fyzických preukazoch. issuerAuth je objekt COSE_Sign1 s alg = ES256 a chráneným záhlavím obsahujúcim x5t [haš parametra záhlavia certifikátu X.509 COSE vymedzený v RFC 9360 (oddiel 2)]; v záujme interoperability sa ako hašovací algoritmus v x5t použije SHA-256).

d) Pred kódovaním QR kódu sa kombinovaný objekt CBOR/COSE **komprimuje pomocou formátu zlib** (RFC 1950, oddiel 2.2) s použitím algoritmu **deflate** (RFC 1951, oddiely 3.2 a 4). Výsledné komprimované bajtové pole sa kóduje v **bajtovom režime QR kódu**, čím sa zabezpečuje plná podpora pre binárne dátové obsahy CBOR/COSE a interoperabilitu skenerov.

Pre všetky textové polia zahrnuté do dátového obsahu QR kódu vydavatelia kódujú znaky v Unicode UTF-8 v rámci textových reťazcov CBOR. Na podpísané údaje dátového obsahu sa neuplatňuje transliterácia. Na účely interoperability vydavatelia pred podpísaním uplatňujú na všetky textové polia normalizačnú formu C (NFC).

e) **Predpona:** Reťazec QR kódu pre európsky preukaz osoby so zdravotným postihnutím sa začína „ED1:MDOC:“. Identifikuje sa tým typ preukazu a kódovací profil. Predpony musia byť prítomné a rozlišujú sa v nich veľké a malé písmená. Neznáme alebo nepodporované predpony vedú k zamietnutiu. Predpona a komprimovaný dátový obsah sa v QR kóde kódujú v bajtovom režime ako jediný dátový segment.

f) **Minimálna veľkosť modulu musí byť ≥ 0,25 mm**, aby sa zabezpečila čitateľnosť na tlačených preukazoch.

g) **Maximálna verzia 20;** s najviac 97 × 97 modulmi na každej strane.

2. **Špecifikácia generovania podpisu pre európsky preukaz osoby so zdravotným postihnutím**

Kvalifikovaná elektronická pečať (QSeal) používaná na zapečatenie QR kódov pre európsky preukaz osoby so zdravotným postihnutím zabezpečuje, že kódované údaje pochádzajú od oprávneného vydávajúceho orgánu a neboli zmenené.

a) **Podpisový algoritmus**: Podpisový algoritmus je ES256 [Elliptic Curve Digital Signature Algorithm (ECDSA) s SHA-256 s použitím krivky P-256], ako sa vymedzuje v RFC 9053 (oddiel 2.1); v COSE je algoritmus identifikovaný parametrom záhlavia alg v RFC 9052 (oddiel 3.1).

b) **Podpisový kľúč**: Dátový obsah QR kódu sa podpisuje pomocou súkromného kľúča zodpovedajúceho kvalifikovanému certifikátu pre elektronickú pečať (QSealC).

c) **Štruktúra COSE:** Podpisový kontajner musí byť objekt COSE_Sign1. Chránené záhlavie musí obsahovať alg (ES256) a x5t [haš parametra záhlavia certifikátu X.509 COSE vymedzený v RFC 9360 (oddiel 2)]; v záujme interoperability sa ako hašovací algoritmus v x5t použije SHA-256). Overovanie sa zakladá na použití hodnoty x5t na lokalizáciu príslušného certifikátu v miestnej vyrovnávacej pamäti úložiska dôvery overovateľa vytvoreného na základe informácií z dôveryhodného zoznamu; následne sa validuje reťazec certifikátov a stav certifikátu v súlade s rámcom dôvery eIDAS.

d) **Podpisový štandard**: Dátový obsah QR kódu musí byť podpísaný ako objekt COSE_Sign1 v súlade s RFC 9052 (oddiel 4), CBOR Object Signing and Encryption. Objekt COSE_Sign1 je obsiahnutý v issuerAuth a musí byť kódovaný bez tagu CBOR pre COSE_Sign1. Pole dátového obsahu objektu COSE_Sign1 musí byť oddelené a kódované ako CBOR null. Na generovanie a overenie podpisu musí byť externým dátovým obsahom štruktúra kódovaná ako deterministický CBOR obsahujúca hodnotu docType a hodnotu issuerSigned z mapy CBOR najvyššej úrovne.

e) **Hašovací algoritmus**: Na generovanie podpisu a overenie integrity sa použije SHA-256 ako súčasť ES256.

f) **Kódovanie**: Dátový obsah sa kóduje pomocou CBOR (RFC 8949, oddiel 4.2), ako sa vyžaduje v špecifikáciách COSE a mDOC, čím sa zabezpečuje kódovanie a reprodukovateľnosť podpísaných údajov.

3. **Špecifikácie pre tlač**

a) **Tichá zóna**: Okolo QR kódu musí byť na všetkých stranách voľný okraj v šírke **štyroch modulov** bez akejkoľvek tlače, vzoru alebo pozadia.

b) **Kontrast**: QR kód musí byť vytlačený na bielom pozadí s minimálnym kontrastným pomerom **4:1**, aby sa zabezpečila vysoká čitateľnosť pri rôznych svetelných podmienkach.

c) QR kód musí byť vytlačený vo farbe vymedzenej v prílohe I k smernici (EÚ) 2024/2841, ktorá zabezpečuje maximálny kontrast.

d) **Umiestnenie a veľkosť**: QR kód vrátane tichej zóny musí mať rozmery 26,25 mm × 26,25 mm a musí byť umiestnený na zadnej strane preukazu v pravom dolnom rohu. QR kód je maximálne vo verzii 20 (97 × 97 modulov) s veľkosťou modulu 0,25 mm alebo väčšou.

QR kód vrátane tichej zóny musí byť umiestnený aspoň 5 mm od pravého okraja a aspoň 5 mm od spodného okraja preukazu.

4. Údaje v QR kóde na európskom preukaze osoby so zdravotným postihnutím

QR kód obsahuje minimálny súbor údajov overiteľný offline v súlade so zásadou minimalizácie údajov stanovenou v článku 5 ods. 1 písm. c) nariadenia (EÚ) 2016/679. Štruktúra dátového obsahu je takáto:

a) Atribúty preukazu sú kódované v CBOR v rámci objektu issuerSigned.

b) Štruktúra je zabalená a podpísaná QSeal vydávajúceho orgánu ako issuerAuth (COSE_Sign1, ES256, vrátane x5t, hašu parametra záhlavia certifikátu X.509 COSE).

c) Výsledný objekt CBOR/COSE sa komprimuje v súlade s bodom 1 písm. d) tejto prílohy. Dátový obsah QR kódu pozostáva z predpony „ED1:MDOC:“, po ktorej nasleduje výsledné komprimované bajtové pole, a úplný dátový obsah sa kóduje v bajtovom režime ako jediný dátový segment QR kódu.

Obsah údajov pozostáva z podsúboru viditeľných údajov z polí na prednej strane preukazu uvedených v prílohe I k smernici (EÚ) 2024/2841 (meno, priezvisko, sériové číslo preukazu, dátum uplynutia platnosti) spolu s identifikátorom zrušenia, elektronickým podpisom a informáciami o schéme.

Elektronický podpis musí obsahovať:

i) issuerAuth – objekt COSE_Sign1 podpísaný **súkromným kľúčom QSealC** vydávajúceho orgánu.

ii) chránené záhlavie, ktoré zahŕňa alg = ES256 (podpisový algoritmus) a x5t (haš parametra záhlavia certifikátu X.509 COSE).

5. Voliteľné údaje

QR kód neobsahuje žiadne voliteľné údaje.

6. Identifikátor zrušenia (RID)

Okrem viditeľného sériového čísla preukazu musí QR kód obsahovať aj vyhradený identifikátor zrušenia (RID).

RID sa používa na určenie stavu zrušenia a na správu zoznamu zrušených preukazov. RID nesmie byť vytlačený na preukaze a nesmie sa zobrazovať overovateľom preukazov.

6.1. *Požiadavky na RID*

RID:

a) musí byť zahrnutý do podpísaného dátového obsahu QR kódu;

b) musí byť jedinečný aspoň v rámci oblasti vydávania vydávajúceho orgánu;

c) nesmie byť vytlačený na preukaze a nesmie byť čitateľný človekom;

d) nesmie odhaľovať osobné údaje a mať priamu výpovednú hodnotu;

e) nesmie byť priamo odvoditeľný z viditeľného sériového čísla preukazu a

f) musí byť kryptograficky viazaný na dátový obsah QR kódu pomocou kvalifikovanej elektronickej pečate.

6.2. *Formát a veľkosť RID*

RID sa kóduje ako bajtový reťazec CBOR (bstr). RID má dĺžku 16 bajtov (128 bitov).

RID vygeneruje vydávajúci orgán pomocou metódy, ktorú má pod kontrolou a ktorá zabezpečuje dostatočnú entropiu a odolnosť voči jeho uhádnutiu alebo vypočítaniu.

6.3. *Zoznamy zrušených preukazov*

Zoznamy zrušených preukazov uverejnené na účely overenia musia odkazovať len na RID zrušených preukazov. Sériové čísla preukazov sa v zoznamoch zrušených preukazov neuverejňujú.

7. Dátový obsah CBOR (vo vnútri QR kódu) európskeho preukazu osoby so zdravotným postihnutím

V dátovom obsahu QR kódu sa zahrnú len nasledujúce údaje v súlade s viditeľnými dátovými poľami európskeho preukazu osoby so zdravotným postihnutím stanovenými v prílohe I k smernici (EÚ) 2024/2841:

Obsah najvyššej úrovne:

a) docType = "eu.edc"

b) issuerSigned.nameSpaces."eu.edc" s atribútmi uvedenými v nasledujúcej tabuľke

c) issuerAuth = COSE_Sign1 (QSeal)

Pole	**Cesta mDOC**	**Typ/formát**
Verzia dátovej schémy	issuerSigned.nameSpaces."eu.edc".ver	reťazec (napr. "1.0")
Typ preukazu: európsky preukaz osoby so zdravotným postihnutím	docType	Enum ("eu.edc")
Sériové číslo preukazu	issuerSigned.nameSpaces."eu.edc".sub	reťazec
Identifikátor zrušenia	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bajtov)
Meno držiteľa preukazu	issuerSigned.nameSpaces."eu.edc".givenName	textový reťazec Unicode (UTF-8)
Priezvisko držiteľa	issuerSigned.nameSpaces."eu.edc".familyName	textový reťazec

preukazu		Unicode (UTF-8)
Dátum uplynutia platnosti preukazu	issuerSigned.nameSpaces."eu.edc".exp	Tag CBOR 1004 v zmysle vymedzenia v RFC 8943 (oddiel 2.1) obsahujúci textový reťazec UTF-8, ktorý predstavuje úplný dátum podľa RFC 3339 vo formáte RRRR-MM-DD.

Elektronický podpis je obsiahnutý v issuerAuth (objekt COSE_Sign1). Reťazec certifikátov nesmie byť vložený v dátovom obsahu QR kódu; namiesto toho musí chránené záhlavie COSE obsahovať x5t, odtlačok certifikátu používaný na lokalizáciu príslušného QSealC vo vyrovnávacej pamäti úložiska dôvery overovateľa.

8. **Príklad dátového obsahu QR kódu na európskom preukaze osoby so zdravotným postihnutím: logická reprezentácia v štýle JavaScript Object Notation s komentármi**

Nasledujúci príklad predstavuje človekom čitateľnú reprezentáciu logického zobrazenia európskeho preukazu osoby so zdravotným postihnutím vo formáte JavaScript Object Notation (JSON). V praxi táto štruktúra nesmie byť čitateľná človekom, pretože:

a) musí byť kódovaná v CBOR (RFC 8949, oddiel 3);

b) musí byť podpísaná pomocou štruktúry COSE_Sign1 bez tagov s oddeleným dátovým obsahom (RFC 9052, oddiel 4);

c) musí zahŕňať dátum uplynutia platnosti ako tag CBOR 1004 s hodnotou úplného dátumu v súlade s RFC 8943 (oddiel 2.1);

d) musí zahŕňať parameter chráneného záhlavia x5t v súlade s RFC 9360 s použitím SHA-256 na QSealC koncového subjektu kódovaný vo formáte DER a

e) musí byť komprimovaná a mať predponu s reťazcom ED1:MDOC: pred zakódovaním do QR kódu.

```
{
  // len človekom čitateľné logické zobrazenie európskeho preukazu osoby so zdravotným postihnutím v štýle JSON.
  // skutočný dátový obsah QR kódu je deterministický CBOR, nie JSON.
  "docType": "eu.edc", // doklad – európsky preukaz osoby so zdravotným postihnutím. Hodnota docType je spolu s
    //issuerSigned zahrnutá v externom dátovom obsahu COSE_Sign1.

  "issuerSigned": {
    // Údaje chránené issuerAuth; použité ako oddelený dátový obsah.
    // Na generovanie a overenie podpisu zahŕňa oddelený externý dátový obsah
    // docType aj issuerSigned.
    "nameSpaces": {
      "eu.edc": {
        "ver": "1.0", // QR profil/verzia schémy

        // Sériové číslo preukazu; vymedzené vydavateľom, maximálne 24 znakov.
```

```
      "sub": "AB123456789012345678 90CD",

      // Identifikátor zrušenia: skutočný CBOR bstr, 16 bajtov/128 bitov.
      // Z dôvodu čitateľnosti tu uvedené ako 32 hexadecimálnych znakov.
      "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      "givenName": "Ann",    // meno vytlačené na európskom preukaze osoby so zdravotným postihnutím
      "familyName": "Other", // priezvisko vytlačené na európskom preukaze osoby so zdravotným postihnutím

      // Skutočné kódovanie CBOR používa tag 1004 pre úplný dátum podľa RFC 3339.
      "exp": "2030-12-31"
    }
  }
 },

 "issuerAuth": {
  // Skutočná forma: COSE_Sign1 bez tagov, nie objekt JSON.
  "type": "COSE_Sign1",
  "tagged": false,       // kódované bez tagu COSE_Sign1 CBOR
  "payload": "detached", // pole dátového obsahu COSE je CBOR null

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

   // x5t: odtlačok certifikátu; parameter záhlavia COSE 34.
```

```
    "x5t": {
      "hashAlg": "SHA-256", // ekvivalentná hašovacia hodnota COSE -16

      // hašovacia funkcia SHA-256 certifikátu QSealC koncového subjektu kódovaného v DER.
      // 32 bajtov reprezentovaných ako 64 hexadecimálnych znakov.
      "hashValue": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  "unprotectedHeader": {}, // v tomto príklade prázdne

  // podpis ES256 COSE: 64 bajtov = 128 hexadecimálnych znakov.
  "signature": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```


9. Používanie kryptografických mechanizmov

Používanie kryptografických mechanizmov v kontexte tejto prílohy musí byť v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA).

PRÍLOHA II

ŠPECIFIKÁCIE QR KÓDU PRE FYZICKÚ VERZIU EURÓPSKEHO PARKOVACIEHO PREUKAZU PRE OSOBY SO ZDRAVOTNÝM POSTIHNUTÍM

1. **Formát QR kódu pre fyzickú verziu európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím**

a) **Formát QR code Model 2** v súlade s medzinárodnými špecifikáciami pre QR kódy ISO/IEC 18004:2024 alebo rovnocennými špecifikáciami.

b) **Úroveň korekcie chýb M** (redundancia 15 %) zabezpečujúca odolnosť vytlačeného QR kódu voči škrabancom alebo voči čiastočnému poškodeniu.

c) **Režim kódovania:** Dátový obsah QR kódu pozostáva z kombinovanej štruktúry issuerSigned Concise Binary Object Representation (CBOR) a zodpovedajúceho objektu podpisu issuerAuth COSE_Sign1 v zmysle vymedzenia v CBOR Object Signing and Encryption (COSE, RFC 9052 oddiely 3.1, 4.2 a 4.4) a zodpovedá vzoru modelu údajov mDOC pre položky issuerSigned, ale prispôsobenému na používanie na statických fyzických preukazoch. issuerAuth je objekt COSE_Sign1 s alg = ES256 a chráneným záhlavím obsahujúcim x5t [haš parametra záhlavia certifikátu X.509 COSE vymedzený v RFC 9360 (oddiel 2)]; v záujme interoperability sa ako hašovací algoritmus v x5t použije SHA-256).

d) Pred kódovaním QR kódu sa kombinovaný objekt CBOR/COSE **komprimuje pomocou formátu zlib (RFC 1950, oddiel 2.2) s použitím algoritmu deflate** (RFC 1951, oddiely 3.2 a 4). Výsledné komprimované bajtové pole sa kóduje v **bajtovom režime QR kódu**, čím sa zabezpečuje plná podpora pre binárne dátové obsahy CBOR/COSE a interoperabilitu skenerov.

Pre všetky textové polia zahrnuté do dátového obsahu QR kódu vydavatelia kódujú znaky v Unicode UTF-8 v rámci textových reťazcov CBOR. Na podpísané údaje dátového obsahu sa neuplatňuje transliterácia. Na účely interoperability vydavatelia pred podpísaním uplatňujú na všetky textové polia normalizačnú formu C (NFC).

e) **Predpona**: Reťazec QR európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím sa začína „EP1:MDOC:“. Identifikuje sa tým typ preukazu a kódovací profil. Predpony musia byť prítomné a rozlišujú sa v nich veľké a malé písmená. Neznáme alebo nepodporované predpony vedú k zamietnutiu. Predpona a komprimovaný dátový obsah sa v QR kóde kódujú v bajtovom režime ako jediný dátový segment.

f) **Minimálna veľkosť modulu musí byť ≥ 0,35 mm**, aby sa zabezpečila čitateľnosť na tlačených preukazoch.

g) **Maximálna verzia 20**; s najviac 97 × 97 modulmi na každej strane.

2. **Špecifikácie generovania podpisu pre európsky parkovací preukaz pre osoby so zdravotným postihnutím**

Kvalifikovaná elektronická pečať (QSeal) používaná na zapečatenie QR kódov pre európsky parkovací preukaz pre osoby so zdravotným postihnutím zabezpečuje, že kódované údaje pochádzajú od oprávneného vydávajúceho orgánu a neboli zmenené.

a) **Podpisový algoritmus**: Podpisový algoritmus je ES256 (ECDSA s SHA-256 s použitím krivky P-256), ako sa vymedzuje v RFC 9053 (oddiel 2.1); v COSE je algoritmus identifikovaný parametrom záhlavia alg v RFC 9052 (oddiel 3.1).

b) **Podpisový kľúč**: Dátový obsah QR kódu sa podpisuje pomocou súkromného kľúča zodpovedajúceho kvalifikovanému certifikátu pre elektronickú pečať (QSealC).

c) **Štruktúra COSE**: Podpisový kontajner musí byť objekt COSE_Sign1. Chránené záhlavie obsahuje alg (ES256) a x5t [haš parametra záhlavia certifikátu X.509 COSE vymedzený v RFC 9360 (oddiel 2)]; v záujme interoperability sa ako hašovací algoritmus v x5t použije SHA-256). Overovanie sa zakladá na použití hodnoty x5t na lokalizáciu príslušného certifikátu v miestnej vyrovnávacej pamäti úložiska dôvery overovateľa vytvoreného na základe informácií z dôveryhodného zoznamu; následne sa validuje reťazec certifikátov a stav certifikátu v súlade s rámcom dôvery eIDAS.

d) **Podpisový štandard**: Dátový obsah QR kódu musí byť podpísaný ako objekt COSE_Sign1 v súlade s RFC 9052 (oddiel 4), CBOR Object Signing and Encryption. Objekt COSE_Sign1 je obsiahnutý v issuerAuth a musí byť kódovaný bez tagu CBOR pre COSE_Sign1. Pole dátového obsahu objektu COSE_Sign1 musí byť oddelené a kódované ako CBOR null. Na generovanie a overenie podpisu musí byť externým dátovým obsahom štruktúra CBOR kódovaná ako deterministický CBOR obsahujúca hodnotu docType a hodnotu issuerSigned z mapy CBOR najvyššej úrovne.

e) **Hašovací algoritmus**: Na generovanie podpisu a overenie integrity sa použije SHA-256 ako súčasť ES256.

f) **Kódovanie**: Dátový obsah sa kóduje pomocou CBOR (RFC 8949, oddiel 4.2), ako sa vyžaduje v špecifikáciách COSE a mDOC, čím sa zabezpečuje kódovanie a reprodukovateľnosť podpísaných údajov.

3. **Špecifikácie pre tlač**

a) **Tichá zóna**: Okolo QR kódu musí byť na všetkých stranách voľný okraj v šírke **štyroch modulov** bez akejkoľvek tlače, vzoru alebo pozadia.

b) **Kontrast**: QR kód musí byť vytlačený na bielom pozadí s minimálnym kontrastným pomerom **4:1**, aby sa zabezpečila vysoká čitateľnosť pri rôznych svetelných podmienkach.

c) QR kód musí byť vytlačený vo farbe vymedzenej v prílohe II k smernici (EÚ) 2024/2841, ktorá zabezpečuje maximálny kontrast.

d) **Umiestnenie a veľkosť:** QR kód vrátane tichej zóny musí mať rozmery **37 mm × 37 mm** a musí byť umiestnený na prednej strane preukazu, mierne vpravo od stredu, smerom k spodnému okraju. QR kód je maximálne vo verzii 20 (97 × 97 modulov) s veľkosťou modulu 0,35 mm alebo väčšou.

QR kód vrátane tichej zóny musí byť umiestnený aspoň 5 mm od spodného okraja preukazu.

4. **Údaje v QR kóde na európskom parkovacom preukaze pre osoby so zdravotným postihnutím**

QR kód obsahuje minimálny súbor údajov overiteľný offline v súlade so zásadou minimalizácie údajov uvedenou v článku 5 ods. 1 písm. c) nariadenia (EÚ) 2016/679. Štruktúra dátového obsahu je takáto:

a) Atribúty preukazu sú kódované v CBOR v rámci objektu issuerSigned.

b) Táto štruktúra je zabalená a podpísaná QSeal vydávajúceho orgánu ako issuerAuth (COSE_Sign1, ES256, vrátane x5t, hašu parametra záhlavia certifikátu X.509 COSE).

c) Výsledný objekt CBOR/COSE sa komprimuje v súlade s bodom 1 písm. d) tejto prílohy. Dátový obsah QR kódu pozostáva z predpony „EP1:MDOC:“, po ktorej nasleduje výsledné komprimované bajtové pole, a úplný dátový obsah sa kóduje v bajtovom režime ako jediný dátový segment QR kódu.

Obsah údajov pozostáva z podsúboru viditeľných údajov z polí na prednej strane preukazu uvedených v prílohe II k smernici (EÚ) 2024/2841 (dátum uplynutia platnosti, sériové číslo preukazu) spolu s identifikátorom zrušenia, elektronickým podpisom a informáciami o schéme.

Elektronický podpis musí obsahovať:

i) issuerAuth – objekt COSE_Sign1 podpísaný **súkromným kľúčom QSealC** vydávajúceho orgánu.

ii) chránené záhlavie, ktoré zahŕňa alg = ES256 (podpisový algoritmus) a x5t (haš parametra záhlavia certifikátu X.509 COSE).

5. Voliteľné údaje

QR kód neobsahuje žiadne voliteľné údaje.

6. Identifikátor zrušenia (RID)

Identifikátor zrušenia európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím musí byť v súlade s bodom 6 prílohy I.

Zoznamy zrušených preukazov pre zrušené európske parkovacie preukazy pre osoby so zdravotným postihnutím musia odkazovať len na RID. Sériové čísla preukazov sa v zoznamoch zrušených preukazov neuverejňujú.

7. Dátový obsah CBOR (vo vnútri QR) európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím

V dátovom obsahu QR kódu sa zahrnú len nasledujúce údaje, ktoré sú v súlade s viditeľnými poľami európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím stanovenými v prílohe II k smernici (EÚ) 2024/2841:

Pole	**Cesta mDOC**	**Typ/formát**
Verzia dátovej schémy	issuerSigned.nameSpaces."eu.epc".ver	reťazec (napr. "1.0")
Typ preukazu:	docType	Enum

európsky parkovací preukaz pre osoby so zdravotným postihnutím		("eu.epc")
Sériové číslo preukazu	issuerSigned.nameSpaces."eu.epc".sub	reťazec
Identifikátor zrušenia	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 bajtov)
Dátum uplynutia platnosti preukazu	issuerSigned.nameSpaces."eu.epc".exp	Tag CBOR 1004 v zmysle vymedzenia v RFC 8943 (oddiel 2.1) obsahujúci textový reťazec UTF-8, ktorý predstavuje úplný dátum podľa RFC 3339 vo formáte RRRR-MM-DD.

Elektronický podpis je obsiahnutý v issuerAuth (objekt COSE_Sign1). Reťazec certifikátov nesmie byť vložený v dátovom obsahu QR kódu; namiesto toho musí chránené záhlavie COSE obsahovať x5t, odtlačok certifikátu používaný na lokalizáciu príslušného QSealC vo vyrovnávacej pamäti úložiska dôvery overovateľa.

8. Príklad dátového obsahu QR kódu na európskom parkovacom preukaze pre osoby so zdravotným postihnutím: logická reprezentácia v štýle JavaScript Object Notation s komentármi

Nasledujúci príklad predstavuje človekom čitateľnú reprezentáciu logického zobrazenia európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím vo formáte JavaScript Object Notation (JSON). V praxi táto štruktúra nesmie byť čitateľná človekom, pretože:

a) musí byť kódovaná v CBOR (RFC 8949, oddiel 3);

b) musí byť podpísaná pomocou štruktúry COSE_Sign1 bez tagov s oddeleným dátovým obsahom (RFC 9052, oddiel 4);

c) musí zahŕňať dátum uplynutia platnosti ako tag CBOR 1004 s hodnotou úplného dátumu v súlade s RFC 8943 (oddiel 2.1);

d) musí zahŕňať parameter chráneného záhlavia x5t v súlade s RFC 9360 s použitím SHA-256 na QSealC koncového subjektu kódovaný vo formáte DER a

e) musí byť komprimovaná a mať predponu s reťazcom EP1:MDOC: pred zakódovaním do QR kódu.

{

// len človekom čitateľné logické zobrazenie európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím, v štýle JSON.

// skutočný dátový obsah QR kódu je deterministický CBOR, nie JSON.

"docType": "eu.epc", // doklad – európsky parkovací preukaz pre osoby so zdravotným postihnutím. Hodnota docType je spolu s

//issuerSigned zahrnutá v externom dátovom obsahu COSE_Sign1.

"issuerSigned": {

// Údaje chránené issuerAuth; použité ako oddelený dátový obsah.

// Na generovanie a overenie podpisu zahŕňa oddelený externý dátový obsah

// docType aj issuerSigned.

"nameSpaces": {

"eu.epc": {

"ver": "1.0", // QR profil/verzia schémy

// Sériové číslo preukazu; vymedzené vydavateľom, maximálne 24 znakov.

"sub": "EF123456789012345678 90GH",

// Identifikátor zrušenia: skutočný CBOR bstr, 16 bajtov/128 bitov.

// Z dôvodu čitateľnosti tu uvedené ako 32 hexadecimálnych znakov.

"rid": "4a8d9c11223344556677 8899aabbccdd",

```
      // Skutočné kódovanie CBOR používa tag 1004 pre úplný dátum podľa RFC 3339.
      "exp": "2030-12-31"
    }
   }
  },

 "issuerAuth": {
  // Skutočná forma: COSE_Sign1 bez tagov, nie objekt JSON.
  "type": "COSE_Sign1",
  "tagged": false,       // kódované bez tagu COSE_Sign1 CBOR
  "payload": "detached", // pole dátového obsahu COSE je CBOR null

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

   // x5t: odtlačok certifikátu; parameter záhlavia COSE 34.
   "x5t": {
    "hashAlg": "SHA-256", // ekvivalentná hašovacia hodnota COSE -16

    // hašovacia funkcia SHA-256 certifikátu QSealC koncového subjektu kódovaného DER.
    // 32 bajtov reprezentovaných ako 64 hexadecimálnych znakov.
    "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
   }
  },

  "unprotectedHeader": {}, // v tomto príklade prázdne
```

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

"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Používanie kryptografických mechanizmov

Používanie kryptografických mechanizmov v kontexte tejto prílohy musí byť v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA).

PRÍLOHA III

OZNAMOVANIE INFORMÁCIÍ UVEDENÝCH V ČLÁNKU 6 ODS. 2

1. Členské štáty poskytujú Komisii nasledujúce informácie o každom príslušnom orgáne alebo subjekte zodpovednom za vydávanie fyzických verzií európskeho preukazu osoby so zdravotným postihnutím alebo európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím:

   a) názov príslušného orgánu alebo subjektu zodpovedného za vydávanie fyzických verzií európskeho preukazu osoby so zdravotným postihnutím alebo európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím;

   b) registračné číslo príslušného orgánu alebo subjektu zodpovedného za vydávanie fyzických verzií európskeho preukazu osoby so zdravotným postihnutím alebo európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím;

   c) kontaktný e-mail a kontaktné telefónne číslo príslušného orgánu alebo subjektu zodpovedného za vydávanie fyzických verzií európskeho preukazu osoby so zdravotným postihnutím alebo európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím;

   d) jeden alebo viac certifikátov, ktoré možno použiť na overenie elektronickej pečate vytvorenej príslušným orgánom alebo subjektom zodpovedným za vydávanie fyzických verzií európskeho preukazu osoby so zdravotným postihnutím alebo európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím, ktoré vydáva, a v prípade ktorých certifikované údaje o totožnosti zahŕňajú názov a registračné číslo vydavateľa, ako sa uvádza v písmene a), resp. v písmene b);

   e) URL miesta, kde vydavateľ uverejňuje stav platnosti fyzických verzií európskeho preukazu osoby so zdravotným postihnutím alebo európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím.

2. Členské štáty môžu Komisii poskytnúť nasledujúce informácie o každom príslušnom orgáne alebo subjekte zodpovednom za vydávanie fyzických verzií európskeho preukazu osoby so zdravotným postihnutím alebo európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím:

   a) URL webovej stránky, ktorá obsahuje pravidlá a podmienky príslušného orgánu alebo subjektu zodpovedného za vydávanie fyzických verzií európskeho preukazu osoby so zdravotným postihnutím alebo európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím, ktoré sa vzťahujú na poskytovanie a používanie fyzických verzií európskeho preukazu osoby so zdravotným postihnutím a európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím, ktoré poskytuje;

   b) v uplatniteľných prípadoch URL webovej stránky, ktorá obsahuje doplňujúce informácie o príslušnom orgáne alebo subjekte zodpovednom za vydávanie fyzických verzií európskeho preukazu osoby so zdravotným postihnutím alebo európskeho parkovacieho preukazu pre osoby so zdravotným postihnutím.

PRÍLOHA IV

TECHNICKÉ ŠPECIFIKÁCIE ZOZNAMU ZNEPLATNENÝCH PREUKAZOV PRE FYZICKÉ VERZIE EURÓPSKEHO PREUKAZU OSOBY SO ZDRAVOTNÝM POSTIHNUTÍM ALEBO EURÓPSKEHO PARKOVACIEHO PREUKAZU PRE OSOBY SO ZDRAVOTNÝM POSTIHNUTÍM

1. Na účely tejto prílohy identifikátor zodpovedá identifikátoru zneplatnenia (RID) vymedzenému v bode 6 prílohy I a v bode 6 prílohy II.

2. Zoznam zrušených preukazov sa vykonáva ako token zoznamu identifikátorov vo formáte CWT (RFC 8392, oddiel 7) v súlade s bodom 5.2 špecifikácie zoznamu statusov tokenov (draft-ietf-oauth-status-list-14) s týmito zmenami:

   a) hodnota tvrdenia type je „application/identifierlist+cwt“;

   b) musí byť uvedené tvrdenie o čase uplynutia platnosti;

   c) tvrdenie StatusList nesmie byť uvedené v súbore tvrdení CWT;

   d) štruktúra IdentifierList vymedzená v bode 3 musí byť uvedená ako tvrdenie v súbore tvrdení CWT pomocou kľúča 65530;

   e) CWT je objekt COSE_Sign1 používajúci na výpočet podpisu podpisový algoritmus v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA);

   f) CWT obsahuje parameter x5chain v zmysle vymedzenia v RFC 9360 (oddiel 2) v chránenom záhlaví, ktoré obsahuje certifikát alebo reťazec certifikátov na overenie podpisu zoznamu zrušených preukazov;

   g) pre podpisový certifikát zoznamu identifikátorov sa môže použiť OID rozšírené použitie kľúča uvedený v špecifikácii zoznamu statusov tokenov (draft-ietf-oauth-status-list-14) a odporúča sa, aby overovatelia podporovali OID rozšírené použitie kľúča uvedený v špecifikácii zoznamu statusov tokenov a aby infraštruktúry vydávajúceho orgánu pri používaní OID rozšírené použitie kľúča uvedeného v špecifikácii zoznamu statusov tokenov nestanovili pole rozšíreného použitia kľúča ako povinné.

3. Štruktúra IdentifierList je štruktúra CBOR s týmto Concise Data Definition Language (CDDL):

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

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

}

Identifier = bstr

Aggregation_uri = tstr